全国计算机技术与软件专业技术资格（水平）考试参考用书

网络工程师考试同步辅导

(上午科目)

工业和信息化部教育与考试中心 推荐

刁爱军 陈海峰 主编 / 赵晗 吴敏 副主编

第4版

清华大学出版社

VISIT…

LANZAROTE Caliente.COM

全国计算机技术与软件专业技术资格(水平)考试参考用书

网络工程师考试同步辅导
(上午科目)(第 4 版)

刁爱军　陈海峰　主　编
赵　晗　吴　敏　副主编

清华大学出版社
北　京

内 容 简 介

本书是按照国家人力资源和社会保障部、工业和信息化部最新颁布的全国计算机技术与软件专业技术资格(水平)考试大纲和指定教材而编写的。全书分为14章，内容包括计算机网络概论、数据通信基础、广域通信网、局域网与城域网、无线通信网、网络互联与互联网、下一代互联网、网络安全、网络操作系统与应用服务器配置、组网技术、网络管理、网络规划和设计、计算机基础知识和计算机专业英语。各章主要从考试大纲要求、考点辅导、典型例题分析和同步练习以及达标训练等方面加以系统的阐释。

本书具有考点分析透彻、例题典型、习题丰富等特点，非常适合备考网络工程师的考生使用，也可作为高等院校或培训班的教材。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

网络工程师考试同步辅导(上午科目)/刁爱军，陈海峰主编. —4版. —北京：清华大学出版社，2018
(全国计算机技术与软件专业技术资格(水平)考试参考用书)

ISBN 978-7-302-50694-2

Ⅰ. ①网…　Ⅱ. ①刁…　②陈…　Ⅲ. ①计算机网络—资格考试—自学参考资料　Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2018)第163097号

责任编辑： 魏　莹　李玉萍
装帧设计： 常雪影
责任校对： 李玉茹
责任印制： 李红英
出版发行： 清华大学出版社
网　　址： http://www.tup.com.cn, http://www.wqbook.com
地　　址： 北京清华大学学研大厦A座　　**邮　　编：** 100084
社 总 机： 010-62770175　　**邮　　购：** 010-62786544
投稿与读者服务： 010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈： 010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载： http://www.tup.com.cn, 010-62791865
印 装 者： 三河市君旺印务有限公司
经　　销： 全国新华书店
开　　本： 185mm×260mm　　**印　张：** 31.25　　**插　页：** 5　　**字　数：** 763千字
版　　次： 2005年6月第1版　2018年9月第4版　　**印　次：** 2018年9月第1次印刷
定　　价： 89.00元

产品编号：071160-01

网络工程师考试(上午)考点分布导航图

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 1 章 计算机网络概论	1.1 计算机网络的形成和发展	作为入门知识，历年真题很少直接考到								①网络拓扑结构； ② IOS OSI/RM； ③ TCP/IP； ④应用层协议； ⑤传输层协议； ⑥网络层协议； ⑦数据链路层协议； ⑧网络分类(LAN、MAN、WAN、接入网、主干网)	**阅读建议** 本章对应《网络工程师教程(第 5 版)》，清华大学出版社出版(以下简称“教程”)。第 1 章“计算机网络概论”，内容的安排与教程基本同步。考生可以对照教程进行同步复习	本章作为入门知识，需要考生了解掌握，历年真题很少直接考查
	1.2 计算机网络的分类和应用											
	1.3 我国互联网的发展											
	1.4 计算机网络体系结构											
	1.5 几种商用网络的体系结构											
	1.6 OSI 协议集											
第 2 章 数据通信基础	2.1 数据通信的基本概念									①PCM、抽样； ②编码； ③通信方式； ④差错控制； ⑤同步控制； ⑥多路复用； ⑦信道特性	**阅读建议** 本章对应教程第 2 章“数据通信基础”。章节的结构安排与教程基本同步，考生可以对照教程进行同步复习	本章考点分值约占总考分的 8%，不同年份所占分值比例又稍有不同，考点相对集中。高频考点为： ◆奈奎斯特采样定理； ◆光纤； ◆调制方式； ◆数据编码； ◆HDLC 协议； ◆循环冗余校验码； ◆海明码
	2.2 信道特性	数据传输时间(1 分)	采样频率(1 分)，香农定理	采样频率(1 分)				采样频率(1 分)，香农定理(2 分)，数据传输时间(2 分)	采样频率(1 分)			
	2.3 传输介质					多模光纤(1 分)						
	2.4 数据编码					数据编码(1 分)						
	2.5 数字调制技术		正交幅度调制(1 分)	正交幅度调制(1 分)	调制技术(1 分)	正交幅度调制(1 分)	DPSK 调制(2 分)		DPSK 调制(2 分)			
	2.6 脉冲编码调制							数据编码(1 分)	数据编码(2 分)			
	2.7 通信方式和交换方式								时分多路复用(1 分)			
	2.8 多路复用技术					T1 载波(1 分)			E1 载波(1 分)			
	2.9 差错控制	海明码(2 分)				海明码(2 分)	CRC 校验码(1 分)	海明码(1 分)				

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 3 章 广域通信网	3.1 公共交换电话网		电路交换网络(1 分)							①帧中继网； ②HDLC 协议	**1. 阅读建议** 本章对应教程第 3 章“广域通信网”。 **2. 贴心提醒** 在教程中并未直接涉及，但在考试中频繁考到	本章考点分值约占总考分的 5%，每年所占分值比较固定。高频考点为： ◆ARQ； ◆帧中继； ◆ATM
	3.2 X.25 公共数据网			HDLC(1 分)			流量控制(1 分)					
	3.3 帧中继网	帧中继网(1 分)							帧中继(1 分)			
	3.4 ISDN 和 ATM		ISDN(2 分)									
第 4 章 局域网与城域网	4.1 局域网技术概论									①以太网； ②网络连接设备； ③VLAN； ④无线 LAN； ⑤CSMA/CA	**1. 阅读建议** 考生可以对照教程相应章节进行同步复习。 **2. 贴心提醒** 章节的结构安排与教程基本同步。考生可以对照教程进行同步复习	本章相关知识点在历次考试中分布相对集中，考点分值约占总考分的 8%。通常考查 IEEE 802.3 标准，VLAN。高频考点为： ◆CSMA/CD 协议； ◆VLAN； ◆IEEE 802.3ae 标准； ◆IEEE 802.11； ◆冲突域与广播域
	4.2 逻辑链路控制子层											
	4.3 IEEE 802.3 标准	动态分配 VLAN(1 分)，VLAN 划分(2 分)	静态分配 VLAN(1 分)；二进制指数后退算法(1 分)	以太网物理地址(1 分)	IEEE 802.1q (1 分)，VLAN (1 分)，CSMA/CD 协议(1 分)	IEEE 802.1q (1 分)；VTP(3 分)；万兆以太网(1 分)	冲突域和广播域(1 分)，VLAN(1 分)，冲突检测(1 分)，网桥、STP(2 分)	千兆以太网标准(1 分)	VLAN(2 分)，MAC 地址漂移(1 分)，帧(1 分)			
	4.4 局域网互联				根交换机(1 分)	局域网互联(1 分)；生成树协议 STP (1 分)	生成树协议 STP (1 分)		生成树协议 STP(1 分)			
	4.5 城域网	Q-in-Q 技术(2 分)	Mac-in-Mac 技术(2 分)									
第 5 章 无线通信网	5.1 移动通信	3G 通信标准(1 分)								①无线局域网 ②移动通信； ③无线个域网； ④无线城域网	**1. 阅读建议** 考生可以对照教程相应章节进行同步复习。 **2. 贴心提醒** 章节的结构安排与教程基本同步，考生可以对照教程进行同步复习	本章考点分值虽然不高，但新增的内容还应作为考试的重点来复习。高频考点为： ◆CSMA/CA 协议； ◆无线局域网标准
	5.2 无线局域网	IEEE 802.11 (1 分)，移动 Ad Hoc 网络(1 分)	AP(1 分)；IEEE 802.11 (1 分)	IEEE802.1x (1 分)；WLAN 的安全(1 分)；移动 Ad Hoc 网络(1 分)		CSMA/CA 协议(1 分)	IEEE802.11 标准(1 分)；CSMA/CA 协议(1 分)；IEEE802.11n 标准(1 分)	IEEE802.11g(1 分)	WLAN 的安全(1 分)			
	5.3 无线个域网		ZigBee 网络(1 分)									
	5.4 无线城域网			4G 移动通信标准(1 分)	4G 标准(1 分)							

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 6 章 网络互联与互联网	6.1 网络互联设备			网桥、交换机(1 分)	集线器、网桥(1 分)					①因特网概念； ②Internet 服务； ③电子商务； ④电子政务； ⑤IP 地址	**1. 阅读提示** 本章对应教程第 6 章“网络互联与互联网”。内容的安排与教程基本同步，只是在章节的结构上做了一些合并与调整。 **2. 贴心提醒** 考生可以对照教程相应章节进行同步复习	本章相关知识点在历次考试中分布相对集中，分值在 20%左右，是考试的重点。通常考查有关路由器与交换机的配置、IP 地址、子网、TCP、IP、网关协议等知识点。高频考点为： ◆IP 地址的划分； ◆RIP； ◆OSPF； ◆路由器和交换机的配置
	6.2 广域网互联											
	6.3 IP 协议	IP 地址(1 分)可用主机地址(2 分),单播地址(1 分)	私网地址(1 分)、子网划分(1 分)，IP 地址(1 分)	主机地址 (1 分)	私网地址(1 分)、分配地址数(1 分)、网络掩码(1 分)、子网划分(1 分)	私网地址(1 分)，主机地址(1 分)汇聚(2 分)	IP 地址(1 分)，主机地址(1 分)，可用主机地址(2 分)	IP 地址(2 分)、可用主机地址(2 分)、子网分配(1 分)、网络掩码(2 分)	主机地址(2 分)、IP 数据报(1 分)、IP 地址(1 分)			
	6.4 ICMP 协议	ICMP 协议(2 分)			ICMP 协议(1 分)				ICMP(1 分)			
	6.5 TCP 协议和 UDP 协议		TCP 连接(1 分)		TCP 连接(2 分)，TCP 协议(1 分)		TCP 连接(1 分)	TCP 连接(2 分)，TCP 拥塞控制(1 分)	UDP(1 分)，TCP(1 分)，TCP 连接(2 分)			
	6.6 域名和地址			DNS (1 分)，ARP 表(1 分)	域名(1 分)，DNS (1 分)	域名解析(3 分)，域名(1 分)	ARP 协议(1 分)，代理 ARP(1 分)，域名解析(1 分)	ARP(1 分)	ARP 表(1 分)、路由表(3 分)			
	6.7 网关协议	RIP 协议(2 分)，OSPF 区域(2 分)	BGP(2 分)，RIPv2(1 分)，路由环路问题(1 分)	RIP(1 分)，RIPv2(1 分)，距离矢量路由协议(1 分)，OSPF 区域(1 分)，OSPF 协议(1 分)，链路状态路由协议(1 分)	BGP(3 分)，OSPF 协议(1 分)	OSPF 区域(1 分)，OSPF 协议(1 分)，路由环路问题(2 分)	路由协议(1 分)，OSPF 协议(1 分)，OSPF 区域(2 分)	RIPv2(1 分)、OSPF 协议(1 分)	OSPF 协议(1 分)，BGP4(2 分)			
	6.8 路由技术	NAT 技术(2 分)CIDR 技术(2 分)	汇聚(1 分)	距离矢量路由协议(1 分)	MPLS(1 分)，汇聚(1 分)，CIDR 技术(2 分)	路由地址(1 分)，汇聚(2 分)	路由汇聚(1 分)		汇聚(1 分)			
	6.9 IP 组播技术	组播地址(2 分)				组播树(1 分)			组播地址(1 分)			

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 6 章 网络互联与互联网	6.10 IP QoS 技术	区分服务(1 分)				RSVP 协议(1 分)						
	6.11 Internet 的应用	HTTP 协议(1 分)			POP3 协议(2 分)	POP3 协议(2 分)	TFTP(1 分)；POP3 协议(2 分)		HTTP、FTP、Telnet(1 分)电子邮件协议(1 分)；HTTPS 协议(1 分)			
第 7 章 下一代互联网	7.1 IPv6	IPv6 地址(1 分)；IPv6 任播地址(1 分)	IPv6 单播地址、任播地址(2 分)	IPv6 地址(1 分)	IPv6 地址(2 分)		IPv6 链路本地地址(1 分)	IPv6 单播地址(2 分)	IPv6 任播地址(1 分)	①IPv6； ②移动 IP	**1. 阅读建议** 考生可以对照教程相应章节进行同步复习。 **2. 贴心提醒** 章节的结构安排与教程基本同步。考生可以对照教程进行同步复习	本章相关知识点在历次考试中分值虽然不高，但是考试必考。高频考点为： ◆IPv6 地址； ◆移动 IP； ◆从 IPv4 向 IPv6 的过渡：隧道技术、双协议栈技术、翻译技术
	7.2 移动 IP	移动 IP(2 分)										
	7.3 从 IPv4 向 IPv6 的过渡		翻译技术(1 分)	隧道技术(1 分)								
	7.4 下一代互联网的发展											

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 8 章 网络安全	8.1 网络安全的基本概念			网络攻击(1 分)	网络攻击(1 分)				网络攻击(1 分)	①私钥加密体制； ②公钥加密体制； ③认证； ④数字签名； ⑤完整性； ⑥访问控制； ⑦安全协议； ⑧病毒防范和入侵检测； ⑨访问控制技术	**阅读建议** 本章对应教程第 8 章“网络安全”。内容的安排与教程基本同步，只是在章节的结构上做了一些合并与调整。考生可以对照教程进行同步复习	本章考点分值约占总考分的 12%。通常考查各类安全技术的功能、原理。高频考点为： ◆数字证书； ◆数字签名； ◆防火墙的功能； ◆ACL； ◆病毒与木马； ◆网络安全协议
	8.2 信息加密技术	AES(1 分)		三重 DES(1 分)		三重 DES(1 分)	三重 DES(1 分)	三重 DES(1 分)； RC5(1 分)； 公钥(1 分)				
	8.3 认证						消息认证(1 分)					
	8.4 数字签名				数字签名(1 分)	数字签名(1 分)	数字签名(1 分)					
	8.5 报文摘要	MD5 (1 分)			MD5 (1 分)	报文认证算法(1 分)		MD5(1 分)； SHA-1(1 分)				
	8.6 数字证书		数字证书(1 分)			数字证书(2 分)						
	8.7 密钥管理											
	8.8 虚拟专用网	IPSec(1 分)			SSL(1 分)			IPSec(1 分)				
	8.9 应用层安全协议		PGP(3 分)， S-HTTP(1 分)	PGP(1 分)； Kerberor 认证(1 分)	S-HTTP、PGP、MIME、SET(1 分)			PGP(1 分)				
	8.10 可信任系统											
	8.11 防火墙	防火墙(1 分)			防火墙(1 分)							
	8.12 病毒防护和入侵检测	入侵检测系统(1 分)		入侵检测系统(1 分)； 病毒(1 分)					入侵检测系统(1 分)； 入侵检测技术(1 分)			

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 9 章 网络操作系统与应用服务器配置	9.1 网络操作系统									①网络操作系统的功能、分类和特点； ②DHCP 服务器的原理和配置； ③DNS； ④WWW； ⑤Windows 2003	**1. 阅读建议** 本章对教程的结构安排做了相应的调整。教程是按照网络服务类型进行分类，而本章则按 Windows 和 Linux 两平台进行分类。考生可以对照教程相应章节进行同步复习。 **2. 贴心提醒** 教程第 9 章“网络操作系统与应用服务器配置”通常以大型应用题的形式在网络工程师考试(下午科目)中考查。但同时在网络工程师考试(上午科目)中有一定涉及。为了避免叙述的重复，本书整理了教程第 9 章的部分考点，内容更详细	本章考点分值约占总考分的 12%。通常考查网络操作系统的功能、Windows 2003 平台下的系统管理和网络应用，高频考点为： ◆IIS 6.0 的功能和配置； ◆Linux 操作系统的命令； ◆DNS 服务的基本原理； ◆WWW 服务的基本原理； ◆FTP 服务的基本原理； ◆电子邮件服务的基本原理； ◆DHCP 服务器的基本原理
	9.2 网络操作系统的基本配置	文件命令(1 分)，用户分组(1 分)	配置目录(1 分)，文件组织(1 分)	文件配置(1 分)，用户组管理(1 分)	文件命令(1 分)	文件命令 (1 分)	文件命令(2 分)，用户分组(1 分)	文件结构(1 分)，文件命令(2 分)，管理远程(1 分)，文件的访问权限(1 分)	文件命令(1 分)、文件配置(1 分)、用户分组(1 分)			
	9.3 Windows Server 2003 IIS 服务的配置		FTP(1 分)	IIS 身份验证(1 分)			FTP 服务器(1 分)					
	9.4 Linux Apache 服务器的配置					Apache 服务器(1 分)	Apache 服务器(1 分)					
	9.5 DNS 服务器的配置	域名(1 分)	DNS 服务器(1 分)、域名服务器(1 分)、域管理(1 分)	域名(1 分)			DNS 服务器(1 分)，域名(1 分)	DNS 服务器(1 分)	域名解析(1 分)；DNS(1 分)；指针(PTR)(1 分)			
	9.6 DHCP 服务器的配置			DHCP 协议(1 分)			DHCP 服务器(2 分)，DHCP 协议(1 分)		DHCP 服务器(1 分)			
	9.7 电子邮件服务器的配置				SMTP(1 分)，配置 POP3 服务器(1 分)							
	9.8 Samba 服务器的配置								Samba 功能(1 分)			
	9.9 Windows Server 2003 安全策略											

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 10 章 组网技术	10.1 交换机和路由器	路由器(2 分)	路由器(1 分)		路由器(1 分)	交换机(1 分)，路由器(1 分)	路由器(1 分)		交换机 (1 分)	①交换机和路由器的配置； ②远程访问服务器； ③多层交换机功能和机制； ④IP 路由器功能和控制	**1. 阅读建议** 本章对应教程的第 10 章"组网技术"，通常以大型应用题的形式在网络工程师考试(下午科目)中考查。 **2. 贴心提醒** 考生可以对照教程相应章节进行同步复习	本章考点分值约占总考分的 8%。通常考查组网技术的相关知识。高频考点为： ◆交换机和路由器的配置； ◆远程访问服务器； ◆多层交换机的功能和机制； ◆IP 路由器的功能和控制
	10.2 交换机的配置		交换机命令(3 分)	交换机配置(1 分)；交换机命令(1 分)	设置交换机的 IP 地址(1 分)		交换机命令(1 分)	VLAN 配置(1 分)；交换机配置(1 分)	交换机配置(1 分)，交换机故障(2 分)			
	10.3 路由器的配置	路由器命令(2 分)		路由器命令(1 分)；路由器连接(1 分)	路由器命令(4 分)		路由器的配置(3 分)	路由器命令(4 分)				
	10.4 配置路由协议			路由器的路由信息 (1 分)；默认路由(1 分)				OSPF 协议(2 分)				
	10.5 配置广域网接入											
	10.6 IPSec 配置与测试											
	10.7 IPv6 配置与部署											
	10.8 访问控制列表		ACL 语句(3 分)	ACL 语句(1 分)								
	10.9 策略路由											

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第11章 网络管理	11.1 网络管理系统体系结构									①网络管理的功能域； ②网络管理协议； ③网络管理工具； ④网络管理平台； ⑤分布式网络管理。 ⑥网络管理命令	**1. 阅读建议** 本章对应教程第 11 章“网络管理”。考生可以对照教程进行同步复习。 **2. 贴心提醒** 本章内容大纲上明确提出，历年考题中有大量考题出现	本章考点分值约占总考分的 8%。通常考查网络管理协议、SNMP 功能及指令、网络管理命令、网络管理工具的使用以及系统可靠性和 RAID 技术。高频考点为： ◆网络管理命令； ◆SNMP 协议； ◆系统可靠性； ◆RAID 技术； ◆NAS 与 SAN
	11.2 网络监控系统的组成											
	11.3 网络管理功能域			故障管理(1 分)								
	11.4 简单网络管理协议	SNMP 协议(1 分)；SNMPv1、SNMPv2(1 分)	SNMPv2(1 分)	SNMP 协议(1 分)；SNMPv3(1 分)	SNMP 管理(1 分)；SNMPv2(1 分)		SNMP 协议(2 分)		SNMP 协议(2 分)			
	11.5 管理数据库 MIB-II											
	11.6 RMON	RMON(1 分)										
	11.7 网络诊断和配置命令	Nslookup (1 分)	网络管理命令(2 分)；Tracert 命令(1 分)；netstat-r(1 分)	ipconfig(1 分)，路由命令(1 分)；Netstat -o(1 分)；ping 命令(1 分)	netstat -n(1 分)；nslookup (2 分)	tracert 命令(1 分)；nslookup (1 分)；Ping 命令(1 分)	arp-d(1 分)	网络检测命令(1 分)	arp-a(1 分)			
	11.8 网络监视和管理工具											
	11.9 网络存储技术								RAID5(1 分)			

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 12 章 网络规划和设计	12.1 结构化布线系统	综合布线(2 分)	综合布线(2 分)				综合布线(2 分)	综合布线(2 分)		①网络系统的需求分析；②网络系统的设计；③通信子网的设计；④资源子网的设计；⑤网络系统的构建和测试	**1. 阅读建议** 考生可完全参看本书复习。 **2. 贴心提醒** 本章内容大纲上明确提出，历年考题中必有考题出现	本章考点分值约占总考分的10%。通常考查网络规划的基础知识。高频考点为：◆网络系统的需求分析；◆布线系统；◆核心交换机；◆资源子网的设计
	12.2 网络分析与设计过程	物理网络设计(1 分)	网络系统生命周期(1 分)；逻辑网络设计(1 分)			物理网络设计(1 分)；逻辑网络设计(1 分)	网络系统设计(1 分)					
	12.3 网络需求分析			网络安全需求(1 分)			网络安全措施(1 分)					
	12.4 通信流量分析											
	12.5 逻辑网络设计											
	12.6 网络结构设计		网络汇聚层(1 分)		网络核心层(1 分)		网络核心层(1 分)	网络接入层(1 分)	网络设计(1 分)			
	12.7 网络故障诊断			网络故障诊断(3 分)	故障诊断(1 分)							
	12.8 网络规划案例	本节属于案例分析，几乎每年都会涉及										

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 13 章 计算机基础知识	13.1 计算机硬件基础	寄存器(1 分)； 定点整数(1 分)； 流水线(2 分)； 内存容量(1 分)	CPU(1 分)； 内存容量(1 分)； 分级存储体系(1 分)	定点小数(1 分)； 存储器(1 分) CPU 中断(1 分) 总线系统(1 分)	DMA(1 分)； 虚拟存储器(1 分)； 寻址方式(1 分)； 内存容量(1 分)	内存容量(1 分)； 总线结构(1 分)	CPU(1 分)； 虚拟存储器(1 分)； 寄存器(1 分)； 浮点数表示(1 分)； 海明码(1 分)； 流水线(1 分)	累加器(1 分)； CPU 可靠性 (1 分)	主存储器(1 分)； cache 与主存的地址映像(1 分)； 流水线技术(1 分)； 中断、DMA(1 分)； 内存容量(1 分)	①计算机部件、指令系统、处理器的性能、存储介质、主存(类型、容量和性能)、主存配置(交叉存取、多级主存)、辅存(容量、性能)、存储系统(虚拟存储器、高速缓存)、中断、DMA、通道、SCSI、I/O 接口与 I/O 设备类型和特征； ②操作系统的功能及分类、多道程序、内核和中断控制、进程和线程、进程的状态及转换、进程调度算法、死锁、存储管理方案、文件管理、作业调度算法； ③需求分析和管理、结构化分析与设计、面向对象分析与设计、模块设计、I/O 设计、人机界面设计、测试评审方法、项目管理基础知识、系统维护； ④安全性标准、相关标准(国际标准、美国标准、国家标准、行业标准与企业标准)、标准化组织、信息化基础知识，远程教育、电子商务、电子政务等基础知识	**1. 阅读建议** 本章内容教程上没有相关内容。考生可完全参看本书复习。 **2. 贴心提醒** 本章内容大纲上明确提出，历年考题中必有考题出现。本书将其整理编排，补充为第 13 章“计算机基础知识”	本章考点分值约占总考分的 10%。 高频考点为： ◆进程调度； ◆文件系统； ◆页式存储； ◆段式存储； ◆PERT 图； ◆甘特图； ◆软件开发方法； ◆软件能力成熟度模型(CMM)； ◆软件版权； ◆著作权； ◆专利权； ◆《标准化法》
	13.2 操作系统	目录结构(2 分)			目录结构(2 分)		PV 操作(1 分)	存储管理(1 分)				
	13.3 系统开发和运行基础	甘特图(2 分)	软件开发方法论(1 分)； PERT(2 分)	语言处理(1 分)； 进程调度(1 分)	PERT 图(2 分)； 软件开发方法论(1 分)	数据流图(2 分)	软件开发方法论(1 分)； PERT(2 分)	PERT(2 分)	PERT(2 分)； 软件开发方法论(1 分)			
	13.4 标准化和信息化	著作权(1 分)	著作权(1 分)	著作权(1 分)	著作权(1 分)	著作权(1 分)	商标法(1 分)	商标法(1 分)； 专利权(1 分)	合理使用 (1 分)			
第 14 章 计算机专业英语	14.1 计算机网络技术基本词汇	不会直接考查词汇，相关考题会结合本章 12.2 节以完形填空的形式出现								①掌握计算机技术的基本英文词汇； ②能正确阅读和理解计算机领域的英文资料； ③具有工程师所要求的英语阅读水平； ④掌握本领域的基本英语词汇	**1. 阅读建议** 本章内容教程上没有相关内容。考生可完全参看本书复习。 **2. 贴心提醒** 本章内容大纲上明确提出，自 2007 年上半年开始每年固定 5 个分值的考题。故本书将其整理编排，补充为第 14 章“专业英语”	本章考点分值每年固定为 5 分，考查范围比较广泛，需要考生广泛阅读
		简单阅读理解(5 分)	简单阅读理解 (5 分)	简单阅读理解 (5 分)	简单阅读理解(5 分)	简单阅读理解 (5 分)	简单阅读理解 (5 分)	简单阅读理解 (5 分)	简单阅读理解 (5 分)			

前　言

全国计算机技术与软件专业技术资格(水平)考试自实施起至今已经历了 20 多年，在社会上产生了很大的影响，其权威性得到社会各界的广泛认可。为了适应我国信息化发展的需求，国家人力资源和社会保障部、工业和信息化部在 2009 年对网络工程师级别考试大纲进行了调整，以满足社会上对各种信息技术人才的需要。本书第 1 版自 2005 年出版以来，被众多考生选用为考试参考书，多次重印，深受广大读者好评。2010 年推出第 2 版。2013 年推出第 3 版。根据网络新技术的发展，为了帮助考生复习迎考，本书结合最新真题和官方教程对第 3 版进行了修订。本书具有如下特色。

(1) 知识点全面。本书与最新网络工程师考试大纲考试科目 1——计算机与网络知识基本一致，又兼顾网络技术发展和知识更新，对属于大纲要求的知识点但指定教材没有阐述的部分进行了必要的补充。

(2) 结构与官方教程同步。本书参考最新指定官方教程、最新考试大纲及最新题型编写章名、节名，便于考生使用《网络工程师教程(第 5 版)》同步复习，同时更加突出重点与难点，针对性强，可减轻考生复习的工作量。

(3) 例题与习题经典。最近 4 年(2014—2017 年)8 次考试真题绝大多数被分类解析到典型例题分析小节中，并且在其中增加了根据考试大纲精心设计的例题，这些例题都具有典型性和代表性，而 2014 年之前的真题则被分类归入同步练习中。使考生能从以前的考题中，更好地熟悉考试的难度与广度，顺利通过考试。

(4) 重点突出。本书沿袭前一版的框架，各章小结之前的几节，基本上分为 4 个模块：考点辅导、典型例题分析、同步练习和同步练习参考答案。其中，考点辅导部分主要以专题的方式，细化网络工程师上午考试各章节的基础知识点的介绍；典型例题分析是本书的重点，它详尽细致地剖析了近 4 年(2014—2017 年)的真题和例题；同步练习的每一道题都配有参考答案；每章还配有一定数量的习题及答案，可对读者所学的知识和能力起到巩固、拓宽和提高的作用。

(5) 对语言进行了锤炼。语言更准确、概念更清晰，覆盖所有大纲考点，并突出重点和难点。

(6) 对所有例题与习题进行了精选。确保所有题目符合考试大纲要求，例题选取更典型、有梯度、有广度，分析详尽；题目的难易度、分布率与真实考试相当；题目答案正确、解析科学。

本书严格按照最新官方指定教材编写，对考生的备考起到事半功倍的效果。

本书非常适合备考网络工程师的考生使用，也可以作为高等院校相关专业或培训班的教材。

本书由刁爱军、陈海峰担任主编，赵晗、吴敏担任副主编。参与本书组织、编写和资料收集的还有谢瑜、周胜、鲁磊纪、杨章静、王华君、陶佳、史国川、徐国明、刘立军、宋白玉、石鲁生、何光明等。

在此对原作品作者及全体参与人员表示衷心的感谢。在本书的编写过程中，参考了许多相关的书籍和资料，从中汲取了许多营养，在此也对这些参考文献的作者表示感谢。需要特别提出感谢的是来自互联网的各位不知道姓名的网友们的无私奉献，正是由于你们，才使本书的内容更完善、更详尽。

由于水平有限，书中难免存在错漏和不妥之处，敬请读者批评指正。联系邮箱：iteditor@126.com。

编　者

目　　录

第 1 章　计算机网络概论........................1

1.1　计算机网络的形成和发展........................1

1.1.1　考点辅导........................1

1.1.2　典型例题分析........................2

1.1.3　同步练习........................2

1.1.4　同步练习参考答案........................2

1.2　计算机网络的分类和应用........................2

1.2.1　考点辅导........................2

1.2.2　典型例题分析........................4

1.2.3　同步练习........................4

1.2.4　同步练习参考答案........................4

1.3　我国互联网的发展........................4

1.3.1　考点辅导........................4

1.3.2　典型例题分析........................5

1.3.3　同步练习........................5

1.3.4　同步练习参考答案........................5

1.4　计算机网络体系结构........................5

1.4.1　考点辅导........................5

1.4.2　典型例题分析........................8

1.4.3　同步练习........................8

1.4.4　同步练习参考答案........................8

1.5　几种商用网络的体系结构........................8

1.5.1　考点辅导........................8

1.5.2　典型例题分析........................9

1.5.3　同步练习........................9

1.5.4　同步练习参考答案........................9

1.6　OSI 协议集........................10

1.6.1　考点辅导........................10

1.6.2　典型例题分析........................11

1.6.3　同步练习........................11

1.6.4　同步练习参考答案........................11

1.7　本章小结........................11

1.8　达标训练题及参考答案........................11

1.8.1　达标训练题........................11

1.8.2　参考答案........................13

第 2 章　数据通信基础........................14

2.1　数据通信的基本概念........................14

2.1.1　考点辅导........................14

2.1.2　典型例题分析........................15

2.1.3　同步练习........................16

2.1.4　同步练习参考答案........................16

2.2　信道特性........................16

2.2.1　考点辅导........................16

2.2.2　典型例题分析........................17

2.2.3　同步练习........................18

2.2.4　同步练习参考答案........................18

2.3　传输介质........................18

2.3.1　考点辅导........................18

2.3.2　典型例题分析........................19

2.3.3　同步练习........................19

2.3.4　同步练习参考答案........................20

2.4　数据编码........................20

2.4.1　考点辅导........................20

2.4.2　典型例题分析........................22

2.4.3　同步练习........................22

2.4.4　同步练习参考答案........................23

2.5　数字调制技术........................23

2.5.1　考点辅导........................23

2.5.2　典型例题分析........................23

2.5.3　同步练习........................24

2.5.4　同步练习参考答案........................24

2.6　脉冲编码调制........................25

2.6.1　考点辅导........................25

2.6.2　典型例题分析........................25

2.6.3　同步练习........................26

2.6.4　同步练习参考答案........................26

2.7　通信方式和交换方式........................26

2.7.1　考点辅导........................26

2.7.2 典型例题分析 28
2.7.3 同步练习 28
2.7.4 同步练习参考答案 29
2.8 多路复用技术 29
2.8.1 考点辅导 29
2.8.2 典型例题分析 30
2.8.3 同步练习 31
2.8.4 同步练习参考答案 31
2.9 差错控制 31
2.9.1 考点辅导 31
2.9.2 典型例题分析 33
2.9.3 同步练习 33
2.9.4 同步练习参考答案 34
2.10 本章小结 34
2.11 达标训练题及参考答案 34
2.11.1 达标训练题 34
2.11.2 参考答案 36

第 3 章 广域通信网 37

3.1 公共交换电话网 37
3.1.1 考点辅导 37
3.1.2 典型例题分析 38
3.1.3 同步练习 39
3.1.4 同步练习参考答案 39
3.2 X.25 公共数据网 39
3.2.1 考点辅导 39
3.2.2 典型例题分析 42
3.2.3 同步练习 43
3.2.4 同步练习参考答案 43
3.3 帧中继网 43
3.3.1 考点辅导 43
3.3.2 典型例题分析 46
3.3.3 同步练习 46
3.3.4 同步练习参考答案 47
3.4 ISDN 和 ATM 47
3.4.1 考点辅导 47
3.4.2 典型例题分析 50
3.4.3 同步练习 50
3.4.4 同步练习参考答案 50
3.5 本章小结 50
3.6 达标训练题及参考答案 51
3.6.1 达标训练题 51
3.6.2 参考答案 53

第 4 章 局域网与城域网 54

4.1 局域网技术概论 54
4.1.1 考点辅导 54
4.1.2 典型例题分析 57
4.1.3 同步练习 57
4.1.4 同步练习参考答案 57
4.2 逻辑链路控制子层 58
4.2.1 考点辅导 58
4.2.2 典型例题分析 59
4.2.3 同步练习 59
4.2.4 同步练习参考答案 60
4.3 IEEE 802.3 标准 60
4.3.1 考点辅导 60
4.3.2 典型例题分析 70
4.3.3 同步练习 72
4.3.4 同步练习参考答案 75
4.4 局域网互联 75
4.4.1 考点辅导 75
4.4.2 典型例题分析 76
4.4.3 同步练习 78
4.4.4 同步练习参考答案 78
4.5 城域网 78
4.5.1 考点辅导 78
4.5.2 典型例题分析 80
4.5.3 同步练习 80
4.5.4 同步练习参考答案 80
4.6 本章小结 80
4.7 达标训练题及参考答案 81
4.7.1 达标训练题 81
4.7.2 参考答案 82

第 5 章 无线通信网 83

5.1 移动通信 83
5.1.1 考点辅导 83

5.1.2 典型例题分析 84
5.1.3 同步练习 85
5.1.4 同步练习参考答案 85
5.2 无线局域网 85
5.2.1 考点辅导 85
5.2.2 典型例题分析 93
5.2.3 同步练习 95
5.2.4 同步练习参考答案 95
5.3 无线个域网 95
5.3.1 考点辅导 95
5.3.2 典型例题分析 99
5.4 无线城域网 100
5.4.1 考点辅导 100
5.4.2 典型例题分析 101
5.4.3 同步练习 102
5.4.4 同步练习参考答案 102
5.5 本章小结 102
5.6 达标训练题及参考答案 103
5.6.1 达标训练题 103
5.6.2 参考答案 103

第 6 章 网络互连与互联网 104

6.1 网络互连设备 104
6.1.1 考点辅导 104
6.1.2 典型例题分析 106
6.1.3 同步练习 106
6.1.4 同步练习参考答案 106
6.2 广域网互联 106
6.2.1 考点辅导 106
6.2.2 典型例题分析 108
6.2.3 同步练习 108
6.2.4 同步练习参考答案 108
6.3 IP 协议 108
6.3.1 考点辅导 108
6.3.2 典型例题分析 113
6.3.3 同步练习 115
6.3.4 同步练习参考答案 116
6.4 ICMP 协议 116
6.4.1 考点辅导 116
6.4.2 典型例题分析 117
6.4.3 同步练习 117
6.4.4 同步练习参考答案 118
6.5 TCP 协议和 UDP 协议 118
6.5.1 考点辅导 118
6.5.2 典型例题分析 119
6.5.3 同步练习 122
6.5.4 同步练习参考答案 122
6.6 域名和地址 122
6.6.1 考点辅导 122
6.6.2 典型例题分析 124
6.6.3 同步练习 127
6.6.4 同步练习参考答案 127
6.7 网关协议 127
6.7.1 考点辅导 127
6.7.2 典型例题分析 129
6.7.3 同步练习 133
6.7.4 同步练习参考答案 134
6.8 路由技术 134
6.8.1 考点辅导 134
6.8.2 典型例题分析 137
6.8.3 同步练习 140
6.8.4 同步练习参考答案 141
6.9 IP 组播技术 141
6.9.1 考点辅导 141
6.9.2 典型例题分析 149
6.9.3 同步练习 149
6.9.4 同步练习参考答案 149
6.10 IP QoS 技术 149
6.10.1 考点辅导 149
6.10.2 典型例题分析 151
6.10.3 同步练习 152
6.10.4 同步练习参考答案 152
6.11 Internet 的应用 152
6.11.1 考点辅导 152
6.11.2 典型例题分析 159
6.11.3 同步练习 160
6.11.4 同步练习参考答案 160
6.12 本章小结 161

6.13 达标训练题及参考答案 161
6.13.1 达标训练题 161
6.13.2 参考答案 166

第 7 章 下一代互联网 168

7.1 IPv6 168
7.1.1 考点辅导 168
7.1.2 典型例题分析 169
7.1.3 同步练习 170
7.1.4 同步练习参考答案 171
7.2 移动 IP 171
7.2.1 考点辅导 171
7.2.2 典型例题分析 173
7.3 从 IPv4 向 IPv6 的过渡 173
7.3.1 考点辅导 173
7.3.2 典型例题分析 176
7.3.3 同步练习 177
7.3.4 同步练习参考答案 177
7.4 下一代互联网的发展 177
7.5 本章小结 178
7.6 达标训练题及参考答案 178
7.6.1 达标训练题 178
7.6.2 参考答案 179

第 8 章 网络安全 180

8.1 网络安全的基本概念 180
8.1.1 考点辅导 180
8.1.2 典型例题分析 182
8.1.3 同步练习 182
8.1.4 同步练习参考答案 182
8.2 信息加密技术 183
8.2.1 考点辅导 183
8.2.2 典型例题分析 185
8.2.3 同步练习 186
8.2.4 同步练习参考答案 186
8.3 认证 186
8.3.1 考点辅导 186
8.3.2 典型例题分析 187
8.3.3 同步练习 188
8.3.4 同步练习参考答案 188
8.4 数字签名 188
8.4.1 考点辅导 188
8.4.2 典型例题分析 189
8.4.3 同步练习 190
8.4.4 同步练习参考答案 191
8.5 报文摘要 191
8.5.1 考点辅导 191
8.5.2 典型例题分析 192
8.5.3 同步练习 192
8.5.4 同步练习参考答案 193
8.6 数字证书 193
8.6.1 考点辅导 193
8.6.2 典型例题分析 194
8.6.3 同步练习 194
8.6.4 同步练习参考答案 194
8.7 密钥管理 195
8.7.1 考点辅导 195
8.7.2 典型例题分析 198
8.7.3 同步练习 198
8.7.4 同步练习参考答案 198
8.8 虚拟专用网 199
8.8.1 考点辅导 199
8.8.2 典型例题分析 203
8.8.3 同步练习 203
8.8.4 同步练习参考答案 203
8.9 应用层安全协议 203
8.9.1 考点辅导 203
8.9.2 典型例题分析 206
8.9.3 同步练习 207
8.9.4 同步练习参考答案 207
8.10 可信任系统 207
8.10.1 考点辅导 207
8.10.2 典型例题分析 209
8.10.3 同步练习 209
8.10.4 同步练习参考答案 209
8.11 防火墙 209
8.11.1 考点辅导 209
8.11.2 典型例题分析 212

8.11.3 同步练习 212
8.11.4 同步练习参考答案 213
8.12 病毒防护 213
8.12.1 考点辅导 213
8.12.2 典型例题分析 214
8.12.3 同步练习 214
8.12.4 同步练习参考答案 214
8.13 入侵检测 214
8.13.1 考点辅导 214
8.13.2 典型例题分析 217
8.13.3 同步练习 218
8.13.4 同步练习参考答案 218
8.14 入侵防御系统 218
8.14.1 考点辅导 218
8.14.2 典型例题分析 219
8.14.3 同步练习 219
8.14.4 同步练习参考答案 219
8.15 本章小结 220
8.16 达标训练题及参考答案 220
8.16.1 达标训练题 220
8.16.2 参考答案 222

第 9 章 网络操作系统与应用服务器配置 223

9.1 网络操作系统 223
9.1.1 考点辅导 223
9.1.2 典型例题分析 225
9.1.3 同步练习 226
9.1.4 同步练习参考答案 226
9.2 网络操作系统的基本配置 226
9.2.1 考点辅导 226
9.2.2 典型例题分析 237
9.2.3 同步练习 238
9.2.4 同步练习参考答案 240
9.3 Windows Server 2008 R2 IIS 服务的配置 240
9.3.1 考点辅导 240
9.3.2 典型例题分析 246
9.3.3 同步练习 247
9.3.4 同步练习参考答案 247
9.4 Linux Apache 服务器的配置 247
9.4.1 考点辅导 247
9.4.2 典型例题分析 250
9.4.3 同步练习 251
9.4.4 同步练习参考答案 251
9.5 DNS 服务器的配置 251
9.5.1 考点辅导 251
9.5.2 典型例题分析 257
9.5.3 同步练习 257
9.5.4 同步练习参考答案 258
9.6 DHCP 服务器的配置 258
9.6.1 考点辅导 258
9.6.2 典型例题分析 266
9.6.3 同步练习 268
9.6.4 同步练习参考答案 269
9.7 Samba 服务器的配置 269
9.7.1 考点辅导 269
9.7.2 典型例题分析 271
9.7.3 同步练习 272
9.7.4 同步练习参考答案 272
9.8 Windows Server 2008 R2 的安全策略 272
9.8.1 考点辅导 272
9.8.2 典型例题分析 272
9.8.3 同步练习 273
9.8.4 同步练习参考答案 273
9.9 本章小结 273
9.10 达标训练题及参考答案 273
9.10.1 达标训练题 273
9.10.2 参考答案 276

第 10 章 组网技术 277

10.1 交换机和路由器 277
10.1.1 考点辅导 277
10.1.2 典型例题分析 279
10.1.3 同步练习 280
10.1.4 同步练习参考答案 280
10.2 交换机的配置 280

10.2.1 考点辅导 280
10.2.2 典型例题分析 286
10.2.3 同步练习 287
10.2.4 同步练习参考答案 288
10.3 路由器的配置 288
10.3.1 考点辅导 288
10.3.2 典型例题分析 294
10.3.3 同步练习 295
10.3.4 同步练习参考答案 296
10.4 配置路由协议 296
10.4.1 考点辅导 296
10.4.2 典型例题分析 302
10.4.3 同步练习 304
10.4.4 同步练习参考答案 305
10.5 配置广域网接入 305
10.5.1 考点辅导 305
10.5.2 典型例题分析 307
10.5.3 同步练习 308
10.5.4 同步练习参考答案 308
10.6 IPSec 配置与测试 308
10.6.1 考点辅导 308
10.6.2 典型例题分析 314
10.6.3 同步练习 314
10.6.4 同步练习参考答案 315
10.7 IPv6 配置与部署 315
10.8 访问控制列表 316
10.8.1 考点辅导 316
10.8.2 典型例题分析 318
10.8.3 同步练习 319
10.8.4 同步练习参考答案 320
10.9 本章小结 320
10.10 达标训练题及参考答案 320
10.10.1 达标训练题 320
10.10.2 参考答案 322

第 11 章 网络管理 323

11.1 网络管理系统体系结构 323
11.1.1 考点辅导 323
11.1.2 典型例题分析 325
11.1.3 同步练习 325
11.1.4 同步练习参考答案 325
11.2 网络监控系统的组成 325
11.2.1 考点辅导 325
11.2.2 典型例题分析 326
11.2.3 同步练习 327
11.2.4 同步练习参考答案 327
11.3 网络管理功能域 327
11.3.1 考点辅导 327
11.3.2 典型例题分析 328
11.3.3 同步练习 328
11.3.4 同步练习参考答案 328
11.4 简单网络管理协议 328
11.4.1 考点辅导 328
11.4.2 典型例题分析 333
11.4.3 同步练习 334
11.4.4 同步练习参考答案 335
11.5 管理数据库 MIB-Ⅱ 335
11.5.1 考点辅导 335
11.5.2 典型例题分析 338
11.5.3 同步练习 338
11.5.4 同步练习参考答案 338
11.6 RMON 338
11.6.1 考点辅导 338
11.6.2 典型例题分析 342
11.6.3 同步练习 343
11.6.4 同步练习参考答案 343
11.7 网络诊断和配置命令 343
11.7.1 考点辅导 343
11.7.2 典型例题分析 350
11.7.3 同步练习 355
11.7.4 同步练习参考答案 355
11.8 网络监视和管理工具 355
11.8.1 考点辅导 355
11.8.2 典型例题分析 359
11.8.3 同步练习 359
11.8.4 同步练习参考答案 360
11.9 网络存储技术 360
11.9.1 考点辅导 360

11.9.2 典型例题分析 362
11.9.3 同步练习 362
11.9.4 同步练习参考答案 362
11.10 本章小结 362
11.11 达标训练题及参考答案 363
11.11.1 达标训练题 363
11.11.2 参考答案 365

第 12 章 网络规划和设计 366

12.1 结构化布线系统 366
12.1.1 考点辅导 366
12.1.2 典型例题分析 368
12.1.3 同步练习 369
12.1.4 同步练习参考答案 369
12.2 网络分析与设计过程 369
12.2.1 考点辅导 369
12.2.2 典型例题分析 371
12.2.3 同步练习 372
12.2.4 同步练习参考答案 372
12.3 网络需求分析 372
12.3.1 考点辅导 372
12.3.2 典型例题分析 374
12.3.3 同步练习 374
12.3.4 同步练习参考答案 375
12.4 通信流量分析 375
12.4.1 考点辅导 375
12.4.2 典型例题分析 376
12.4.3 同步练习 376
12.4.4 同步练习参考答案 376
12.5 逻辑网络设计 376
12.5.1 考点辅导 376
12.5.2 典型例题分析 377
12.5.3 同步练习 378
12.5.4 同步练习参考答案 378
12.6 网络结构设计 378
12.6.1 考点辅导 378
12.6.2 典型例题分析 390
12.6.3 同步练习 392
12.6.4 同步练习参考答案 393
12.7 网络故障诊断 393
12.7.1 考点辅导 393
12.7.2 典型例题分析 395
12.7.3 同步练习 397
12.7.4 同步练习参考答案 397
12.8 网络规划案例 397
12.8.1 考点辅导 397
12.8.2 典型例题分析 398
12.8.3 同步练习 398
12.8.4 同步练习参考答案 398
12.9 本章小结 398
12.10 达标训练题及参考答案 398
12.10.1 达标训练题 398
12.10.2 参考答案 399

第 13 章 计算机基础知识 400

13.1 计算机硬件基础 400
13.1.1 考点辅导 400
13.1.2 典型例题分析 407
13.1.3 同步练习 412
13.1.4 同步练习参考答案 413
13.2 操作系统 413
13.2.1 考点辅导 413
13.2.2 典型例题分析 421
13.2.3 同步练习 422
13.2.4 同步练习参考答案 424
13.3 系统开发和运行基础 424
13.3.1 考点辅导 424
13.3.2 典型例题分析 432
13.3.3 同步练习 434
13.3.4 同步练习参考答案 435
13.4 标准化和信息化 435
13.4.1 考点辅导 435
13.4.2 典型例题分析 438
13.4.3 同步练习 440
13.4.4 同步练习参考答案 440
13.5 本章小结 440
13.6 达标训练题及参考答案 441
13.6.1 达标训练题 441

13.6.2　参考答案 444

第 14 章　计算机专业英语 445

14.1　计算机网络技术基本词汇 445

14.2　专业英语试题分析 475

14.2.1　考点辅导 475

14.2.2　典型例题分析 477

14.2.3　同步练习 480

14.2.4　同步练习参考答案 481

14.3　本章小结 481

14.4　达标训练题及参考答案 481

14.4.1　达标训练题 481

14.4.2　参考答案 483

参考文献 485

第 1 章　计算机网络概论

大纲要求：

- 网络拓扑结构。
- 网络分类(LAN、MAN、WAN、接入网、主干网)。
- OSI/RM。
- TCP/IP 协议簇，包括应用层协议、传输层协议(TCP、UDP)、网络层协议(IP)、数据链路层协议。

1.1　计算机网络的形成和发展

1.1.1　考点辅导

计算机网络是指由通信线路连接的许多自主工作的计算机构成的集合体。这里强调构成网络的计算机是自主工作的，是为了和多终端分时系统相区别。在计算机网络中的各个计算机(工作站)本身拥有计算机资源，能独立工作，完成一定的任务，同时还可以使用网络中其他计算机的资源(如 CPU、大容量外存或信息等)。

1. 早期的计算机网络

早期的计算机网络出现在 20 世纪 50 年代，它实际上是以单个计算机为中心的远程联机系统。在这种系统中，除了一台中心计算机，其余的终端不具备自主处理能力。这种网络也称为面向终端的计算机网络。

2. 现代计算机网络的发展

20 世纪 60 年代中期出现了以多个大型主机为中心的网络，典型代表是 ARPANET。该时期的计算机网络是多台主机通过通信线路连接起来的，它和以单台计算机为中心的远程联机系统的主要区别是，在这种网络中每台计算机都有独立的处理能力，在这些机器之间不存在主从关系。但是由于该时期的计算机网络是由研究单位、大学等部门各自研制的，没有统一的网络体系结构，因此要把这些计算机连接起来很困难。

3. 计算机网络标准化阶段

1977 年，国际标准化组织(ISO)的 TC97 信息处理系统技术委员会 SC16 分技术委员会开始着手制定开放系统互连参考模型(OSI/RM)。作为国际标准，OSI 规定了可以互相连接(简称互连或互联)的计算机系统之间的通信协议，遵从 OSI 协议的网络通信产品都是“开放系统”。这种网络具有统一的网络体系结构，能够很方便地把不同的计算机连接起来。

4. 微型机局域网的发展时期

20世纪80年代初期出现了微型计算机。1972年，Xerox公司发明了以太网，以太网与微型机的结合使得微型机局域网得到了快速的发展。1980年2月，IEEE组织了一个802委员会，开始制定局域网标准。

5. 国际互联网的发展时期

20世纪90年代开始，各种网络技术融合在了一起。该时期网络的特点是高速化和综合化。Internet(因特网，又称国际互联网)以惊人的高速度发展，网上的主机数量、上网人数、网络的信息流量每年都在迅速增长。

1.1.2 典型例题分析

例1-1 早期的计算机网络是由________组成的。

A. 计算机、通信线路、计算机　　B. PC、通信线路、PC

C. 终端、通信线路、终端　　D. 计算机、通信线路、终端

解析：早期的计算机网络是面向终端的计算机网络，在这种网络中主要存在的是终端和中心计算机进行通信。

答案：D

1.1.3 同步练习

1. 计算机网络系统是由________子网和________子网组成。

A. 通信、资源　　B. 通信、I/O

C. I/O、资源　　D. 主机、I/O

2. 组建计算机网络的目的是实现联网计算机系统的________。

A. 硬件共享　　B. 软件共享

C. 数据共享　　D. 资源共享

1.1.4 同步练习参考答案

1. A　　2. D

1.2 计算机网络的分类和应用

1.2.1 考点辅导

1. 计算机网络的分类

计算机网络一般有以下几种分类方式。

- 按地域范围，可分为局域网(LAN)、城域网(MAN)和广域网(WAN)3 类。
- 按网络拓扑结构，可分为总线型、星型、环型、网状型等。
- 按所采用网络协议的不同，可分为 TCP/IP 网络、SPX/IPX 网络等。
- 按交换方式，可分为电路交换网、分组交换网、帧中继交换网、信源交换网等。
- 按通信介质，可分为有线网和无线网。
- 按网络控制方式，可分为集中式和分布式。

计算机网络的组成元素可以分为两大类，即网络节点和通信链路。网络节点又可分为端节点和转接节点。端节点指信源和信宿节点，如用户主机和用户终端；转接节点指网络通信过程中起控制和转发信息作用的节点，如交换机、集线器、接口信息处理机等。通信链路是指传输信息的信道，可以是电话线、同轴电缆、无线电线路、卫星线路、微波中继线路、光纤缆线等。网络节点通过通信链路连接成的计算机网络如图 1-1 所示。

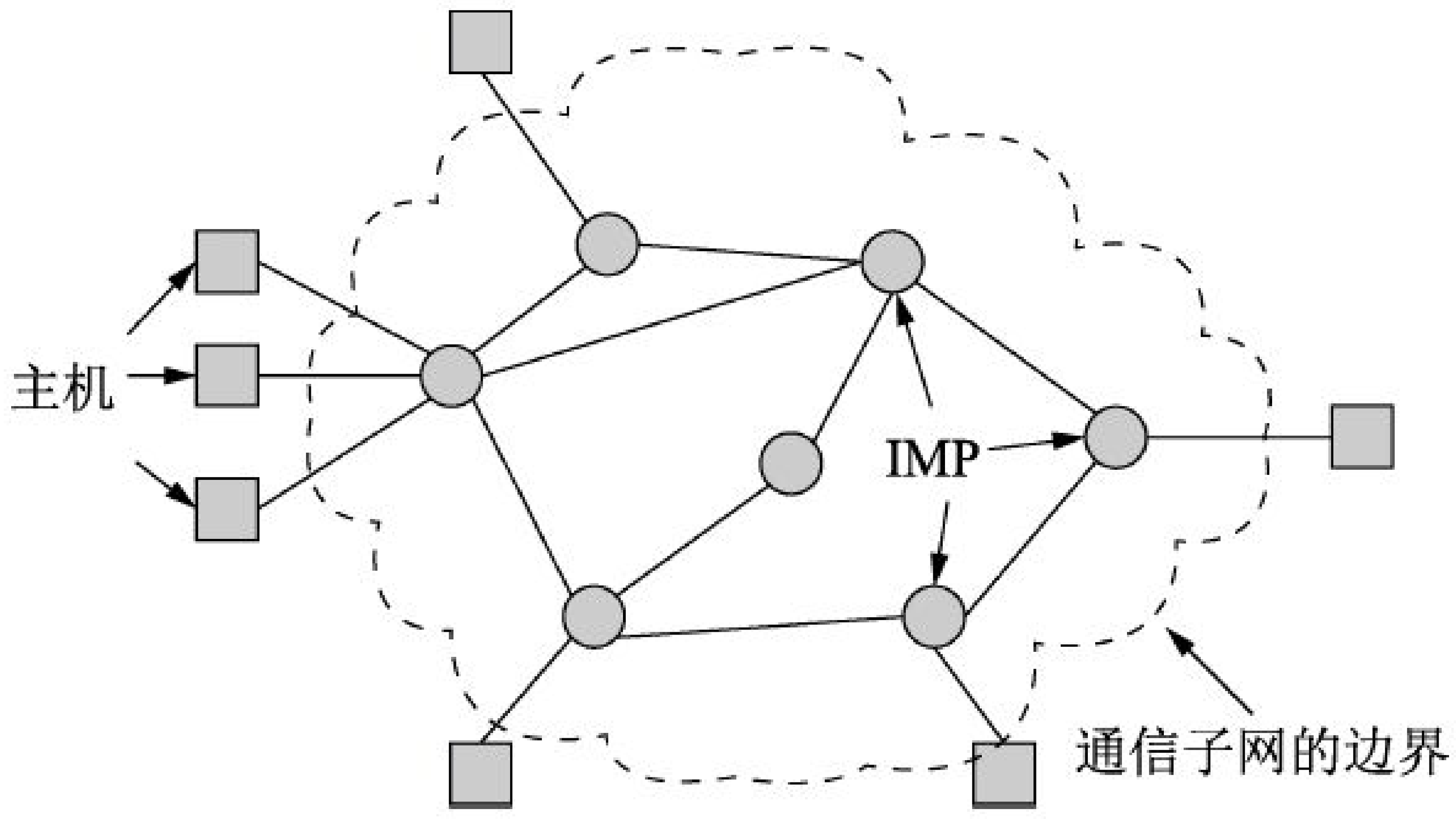


图 1-1　通信子网与资源子网

在图 1-1 中，虚线框外的部分称为资源子网。资源子网包括拥有资源的用户主机和请求资源的用户终端，它们都是端节点。虚线框内的部分称为通信子网，其任务是在端节点之间传送由信息组成的报文，主要由转接节点和通信链路组成。接口信息处理机(Interface Message Processor，IMP)是一种专用通信的计算机。

通信子网中转发节点的互连模式称为子网的拓扑结构。

- 点—点线路(也称为点对点线路)通信子网。即每条物理线路连接一对节点。采用点—点线路的通信子网的基本拓扑结构有星型、环型、树型与网状型。
- 广播信道通信子网。即所有网络节点共享一个公共的通信信道。采用广播信道的通信子网的基本拓扑结构有总线型、树型、环型、无线通信与卫星通信。

2. 计算机网络的应用

计算机网络的应用涉及社会生活的各个方面。当前，对人们的经济和文化生活影响最大的网络应用如下。

- 办公自动化。
- 电子数据交换。
- 远程教育。
- 电子银行。
- 证券和期货交易。
- 娱乐和在线游戏。

1.2.2 典型例题分析

例 1-2 下列拓扑结构中不采用点—点线路的通信子网是________。

A. 星型　　B. 环型　　C. 树型　　D. 总线型

解析：采用点—点线路的通信子网的基本拓扑结构有星型、环型、树型与网状型，而总线型通常采用广播信道通信子网。

答案：D

1.2.3 同步练习

________结构要求把工作站连接到一台中央设备。

A. 星型　　B. 环型

C. 树型　　D. 总线型

1.2.4 同步练习参考答案

A

1.3 我国互联网的发展

1.3.1 考点辅导

1. 我国互联网的建设

2017 年 1 月 22 日下午，中国互联网网络信息中心(CNNIC)发布第 39 次《中国互联网络发展状况统计报告》。截至 2016 年 12 月，中国网民规模达 7.31 亿，相当于欧洲人口总量，互联网普及率达到 53.2%，超过全球平均水平 3.1 个百分点，超过亚洲平均水平 7.6 个百分点。截至 2016 年 12 月，我国手机网民规模达 6.95 亿，增长率连续三年超过 10%。台式电脑、笔记本电脑的使用率均出现下降，手机不断挤占其他个人上网设备的使用。

2. 我国建成的互联网

- 中国公用计算机互联网(CHINANET)。
- 中国教育科研网(CERNET)。
- 中国科学技术网(CSTNET)。
- 中国金桥信息网(CHINAGBN)。

1.3.2　典型例题分析

例 1-3　下列________不是我国建成的主干网。

A. CHINANET　　B. CSTNET　　C. CHINAGBN　　D. USANET

解析：我国建成的互联网有中国公用计算机互联网(CHINANET)、中国教育科研网(CERNET)、中国科学技术网(CSTNET)和中国金桥信息网(CHINAGBN)。

答案：D

1.3.3　同步练习

我国互联网的发展启蒙于________。

A. 20 世纪 80 年代末　　B. 20 世纪 70 年代末

C. 20 世纪 60 年代末　　D. 20 世纪 50 年代末

1.3.4　同步练习参考答案

A

1.4　计算机网络体系结构

1.4.1　考点辅导

1.4.1.1　计算机网络的功能特性

计算机网络应在源节点和目标节点之间提供传输线路，这种传输线路可能要经过一些中间节点。计算机通信有一个特点，即间歇性或突发性。计算机网络的设计者发明了一些新的交换技术来满足这种特殊的通信要求。计算机网络的功能之一是对传输的信息流进行分组，加入控制信息，并把分组正确地传送到目的地。

加入分组的控制信息主要有两种：一种是接收端用于验证是否正确接收到差错控制信息；另一种是指明数据包的发送端和接收端的地址信息。另外，当多个节点同时要求发送分组时，网络还必须通过某种冲突仲裁过程决定谁先发送谁后发送。所有这些带有控制信息的数据包在网络中通过一个个节点正确向前传送的功能称为数据链路控制(DLC)功能。

网络的通信是相当复杂的，涉及一系列相互作用的功能过程，把实现复杂的网络通信过程的各种功能划分成层次结构，就是网络的分层体系结构。

1.4.1.2　开放系统互连参考模型的基本概念

开放系统是指遵从国际标准、能够通过互联(也称为互连)而相互作用的系统。显然，系

统之间的相互作用只涉及系统的外部行为，而与系统内部的结构和功能无关。因而关于互连系统的任何标准都只是关于系统外部特性的规定。

OSI/RM(开放系统互连参考模型)是一种分层的体系结构。从逻辑功能看，每一个开放系统都是由一些连续的子系统组成，这些子系统处于各个开放系统和分层的交叉点上，一个层次由所有互联系统的同一层上的子系统组成。

1. OSI/RM 的设计原理

1) 分解

为了实现计算机之间的通信，必须考虑众多的因素。解决复杂问题的最佳方法就是分解，将整个系统划分为若干易于实现和控制的子模块，并通过对各个子模块的功能、交换的数据结构和时序进行约定，协调模块之间的动作，保证系统设计的合理性和互操作性。同时可以根据各子模块的依赖关系，使用结构化的设计和实现方法，采用具有层次结构的模型与之对应。

2) 抽象

标准的提出应当独立于实现的具体环境，为此，OSI/RM 确立采用三级抽象技术。

首先，提出 OSI/RM(第一级抽象)，建立计算机网络在概念和功能上的框架，包括确定 OSI 的层次模型，以及公共术语、属性和子模块的功能等。该框架应能适应新技术的发展和新应用的要求。

其次，提出 OSI 服务定义(第二级抽象)，在 OSI/RM 的基础上，定义各个子模块可提供的服务(即确定各个子模块的外观特性)。

最后，定义 OSI 协议规范(第三级抽象)，定义了一组为确保子模块服务的提供而应遵循的规则。这组规则称为协议，包括确定语法(规定通信双方交换的数据格式、编码和电平信号等)、语义(规定用于协调双方动作的信息及其含义等)和时序(规定动作的时间、速度匹配和事件发生的顺序等)。协议本身并未硬性规定具体的实现技术，因此为协议的实现者保留了充分的灵活性。

3) 子模块(层)划分的原则

各子模块具有相对的独立性，模块之间交互的信息尽可能少，从而尽可能地减少模块之间的依赖性。子模块之间遵循单向引用的原则，使得 OSI/RM 呈现出层次的结构。不同的子模块分属于不同的层次，上层的模块引用下层模块提供的服务。各个层次在使用下层服务的基础上，完成特定的通信功能，向更高层提供增值服务。

分层原则具有以下特点。

- 互联的系统必须具有相同的层次结构。
- 只有相同层次的实体(功能的实施者)才能进行有意义的通信，并且这种通信只能借助于其下层的服务来实现。

4) OSI 的层次

层次的划分是在逻辑上对通信功能的划分。层次不能太少，以使每个层次易于实现和管理；层次也不能太多，否则汇集各层功能的开销太大。ISO 在上述分层的基础上，将 OSI/RM 定义为 7 个层次，自下而上分别如下。

- 物理层(PHL)：确定物理设备接口，提供点—点的二进制位流传输的物理链路。

- 数据链路层(DLL)：利用差错处理技术，提供高可靠传输的数据链路。
- 网络层(NL)：利用路由技术，实现用户数据的端—端传输。
- 传输层(TL)：屏蔽子网差异，以及用户要求和网络服务之间的差异。
- 会话层(SL)：提供控制会话和数据传输的手段。
- 表示层(PL)：解决异种系统之间的信息表示问题，屏蔽不同系统在数据表示方面的差异。
- 应用层(AL)：利用下层的服务，满足具体的应用要求。

2. OSI/RM 的重要概念

1)　协议和服务的区别及相互关系

在开放系统互连参考模型(OSI/RM)中采用了 7 层协议体系结构，除最高层和最低层以外的任何一层，均可记为(*N*)，表示“第 *N* 层”。

在 OSI/RM 模型中，协议和服务是两个非常重要的不同的概念。控制两个 *N* 层对等实体进行通信的规则的集合称为(*N*)协议；两个 *N* 层实体间的通信在(*N*)协议的控制下，能够使 *N* 层向上一层提供服务，这种服务就称为(*N*)服务，接受(*N*)服务的 *N* 层服务用户是 *N*+1 层实体。

2)　服务访问点

服务访问点(Service Access Point，SAP)是指同一系统中相邻两层实体之间进行交换信息之处，即 *N* 层实体和 *N*+1 层实体之间的逻辑接口，也称为插口(Socket)或端口(Port)。一个 *N* 层服务是由一个 *N* 层实体作用在一个 *N* 层 SAP 上来完成的，虽然两层之间可以允许有多个 SAP，但一个 *N* 层 SAP 只能被一个 *N*+1 层实体所使用；但一个 *N* 层实体却可以向多个 *N* 层 SAP 提供服务，这称为连接复用；一个 *N*+1 层实体也可以使用多个 *N* 层 SAP，这称为连接分裂。

3)　数据单元

OSI 环境中的数据交换主要发生在层与层之间，被交换的数据总称为数据单元(DU)。

相邻层间交换的数据单元称为服务数据单元(SDU)。SDU 可以被理解为服务原语的表现形式。

相邻层接口之间传送的数据单元称为接口数据单元(IDU)。IDU 包含 SDU 以及部分用于相邻实体区分和识别的接口控制信息(ICI)。

对等层间交换的数据单元称为协议数据单元(PDU)。为了保证系统的开放性和互操作性，PDU 的内容和格式由协议精确地定义。通常(*N*)PDU 作为(*N*−1)SDU 的一部分传递给下层，直至对等层实体。

4)　服务原语

服务原语(Service Primitive)是指服务用户与服务提供者之间进行交互时所要交换的一些必要信息。服务原语由原语名和原语参数两部分组成，可分为无确认的服务原语和有确认的服务原语两种。服务原语的特点是它的处理应具有原语的特征，即原语执行的过程不允许被中断，或者被中断原语的执行应和原语的连续执行具有完全相同的结果。

3. OSI/RM 特点分析

OSI/RM 的概念比较抽象，它并没有规定具体的实现方法和措施，更未对网络的性能提

出具体的要求，而只是一个为制定标准用的概念性框架。OSI/RM的7层协议模型上下大，中间小，这是因为最高层要和各种类型的应用进程接口，而最低层要和各种类型的网络接口，因此上、下两头标准特别多，而中间几层标准就稍简单些。有些层的任务过于繁重，如数据链路层和网络层；有些层的任务又太轻，如会话层和表示层。

1.4.2　典型例题分析

例 1-4　下列不是OSI/RM确立采用的三级抽象技术的是________。

A. OSI/RM　　B. OSI服务定义　　C. OSI协议规范　　D. OSI分层定义

解析：标准的提出应当独立于实现的具体环境，为此，OSI/RM确立采用三级抽象技术。首先提出OSI/RM(第一级抽象)，建立计算机网络在概念和功能上的框架，包括确定OSI的层次模型；其次提出OSI服务定义(第二级抽象)；最后定义OSI协议规范(第三级抽象)，定义了一组为确保子模块服务的提供而应遵循的规则。

答案：D

1.4.3　同步练习

相邻层间交换的数据单元称为________。

A. SDU　　B. IDU　　C. ICI　　D. PDU

1.4.4　同步练习参考答案

A

1.5　几种商用网络的体系结构

1.5.1　考点辅导

1. SNA

1974年，IBM公司推出了系统网络体系结构，这是一种以大型主机为中心的集中式网络。SNA协议分为7层：物理层、数据链路控制层、路径控制层、传输控制层、数据流控制层、表示服务层、事务处理服务层。随着计算机局域网的广泛使用，IBM推出了第二代的高级点对点网络(APPN)，使得SNA由集中式网络演变成点对点的网络环境。在APPN网络环境中有下面3类节点。

(1)　低级入口节点(LEN)。这种节点只能利用与其相连的网络节点提供的服务进行会话。

(2)　端节点(EN)。这种节点包含APPN的部分功能，还具有路由能力，能够通过网络

节点与其他端节点建立会话。

(3)　网络节点(NN)。这种节点包含 APPN 的全部功能，其中的控制点(CP)功能管理着 NN 的全部资源，能够建立 CP—CP 会话，维护网络的拓扑结构，并提供目录服务。

2. X.25

X.25 是 CCITT 在 1976 年公布的公用数据网(PDN)标准，后来又经过了两次修订。X.25 包括了通信子网最下边的 3 个逻辑功能层，即物理层、数据链路层和网络层，与 SNA 下面 3 层是对应的。

最低层用 X.21 作为用户节点(DTE)和通信子网之间建立电气连接的对等协议。虚电路连接(VC)的建立和释放既关系到端对端的功能特性，也关系到端节点对网络的功能特性。

3. Novell NetWare

目前市场上流行的版本是 NetWare 4.2。Novell 公司的专用通信协议是 IPX/SPX。IPX 是 Novell 公司按照 Xerox 公司的 IDP 协议实现的网络层协议，提供无连接的数据报服务，用于工作站和服务器之间传送数据。SPX 是 Novell 公司的传输层协议，在分布式应用之间提供顺序提交服务。

NetWare 核心协议(NCP)管理服务器资源，它向服务器发出过程调用来使用文件和打印资源。突发模式协议(BMP)是为提高文件传输的效率而设计的。用突发模式通信，允许对一个请求发回多个响应包。NetWare 目录服务(NDS)是一个分布式网络数据库。在基于 NDS 的网络中，仅需一次登录就可以访问所有的服务器，而以前基于装订库的网络则需要在不同的服务器之间不断切换。

1.5.2　典型例题分析

例 1-5　下面不属于 APPN 网络环境中的三类节点的是________。

A. LEN　　B. EN　　C. NN　　D. SEN

解析： 在 APPN 网络环境中有下面三类节点：低级入口节点(LEN)、端节点(EN)、网络节点(NN)。

答案： D

1.5.3　同步练习

下列不是 X.25 包括的通信子网最下边的 3 个逻辑功能层的是________。

A. 物理层　　B. 数据链路层　　C. 网络层　　D. 传输控制层

1.5.4　同步练习参考答案

D

1.6 OSI 协议集

1.6.1 考点辅导

1. 物理层协议

在物理层，OSI 采用了各种现成的协议，其中有 RS-232、RS-449、X.21、X.35、ISDN，以及 FDDI、IEEE 802.3、IEEE 802.4 和 IEEE 802.5 的物理层协议。

2. 数据链路层协议

在数据链路层，OSI 的协议集也是采纳了当前流行的协议，其中包括 HDLC、LAP-B 以及 IEEE 802 的数据链路层协议(ISO 8802)。

3. 网络层协议

网络层提供两种服务，即面向连接的服务和无连接的服务。ISO 8348 文件定义了面向连接的服务(CONS)，与此对应的协议是 CCITT X.213，这两个文件的规定与 X.25 分组级协议(PLP)一致。ISO 8473 文件定义了无连接的网络服务(CLNS)。在 OSI 参考模型中，各个层次除了服务定义文件外，还有定义该功能的协议规范文件，但是在网络层没有相应的协议规范文件。

ISO 8878 文件(或 X.223)类似于网络层的协议规范，它规定了从 X.213 服务原语到 X.25 分组协议的映像关系。

另外，关于网际互联，ISO 9542 描述了端系统和中间系统(ES-IS)之间的通信协议，ISO 10589 描述了中间系统与中间系统(IS-IS)之间的通信协议。

4. 传输层协议

面向连接的传输层协议分为 5 类，即 TP0、TP1、TP2、TP3 和 TP4。这 5 类传输协议在不同的通信子网服务的基础上都能提供完整的数据传送，组网时可根据子网的情况选用。

5. 会话层协议

OSI 会话层协议是在 ECMA 提供的会话协议和 CCITT 的 T.62(Teletex)建议的基础上制定的，它既包含了面向计算机应用的功能，也包含了与智能用户电报(Teletex)兼容的功能。

6. 表示层协议

OSI 表示层服务定义文件 ISO 8822(CCITT X.209)描述了一种具体的编码规则，叫作传送语法。OSI 表示层服务定义文件是 ISO 8822(CCITT X.216)，协议规范文件是 ISO 8823(CCITT X.226)。表示层过程用于建立连接、控制数据的发送和同步。它只是一个很简单的相邻层之间的“过路”协议。

7. 应用层协议

应用层是 OSI 的最高层，这一层的协议都与应用进程间的通信有关。已经定义的 OSI

应用层协议主要有 5 种：OSI 的电子邮件标准(ISO 10021)叫作 MOTIS，它是根据 CCITT 的 X.400 建议制定的；OSI 的文件传输协议(ISO 8571 和 ISO 8572)叫作 FTAM，这是一个适用于各种文件类型的功能很强的文件访问协议；OSI 的目录服务(DS)协议来源于 CCITTR X.500 系列协议，提供分布式数据库功能；OSI 的虚拟终端(VT)协议定义了表示实际终端抽象状态的数据结构，用于解决各种终端不兼容的问题；关于网络管理，OSI 指定了公共管理协议(CMIP)和公共管理信息服务(CMIS)。

1.6.2　典型例题分析

例 1-6　下列是 OSI 的文件传输协议的是________。

A. FTAM　　B. MOTIS　　C. DS　　D. VT

解析：OSI 的文件传输协议(ISO 8571 和 ISO 8572)叫作 FTAM。

答案：A

1.6.3　同步练习

用于建立连接、控制数据的发送和同步的是________。

A. 网络层　　B. 会话层　　C. 表示层　　D. 应用层

1.6.4　同步练习参考答案

C

1.7　本 章 小 结

本章知识点在 2009 年的新大纲中基本没有改变，只是一些表述方式的调整。

本章主要要求考生掌握计算机网络的基本概念、OSI/RM 协议，了解互联网的发展。由于上午考试也会涉及网络系统设计(属于下午考试大纲内容)方面的内容，所以本章在 1.5 节额外添加了几种商用网络的体系结构，供考生参考。

本章相关知识点在历次考试中都会有所涉及，分值在 3 分左右。为了使考生更好地掌握考点，本章前几节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

1.8　达标训练题及参考答案

1.8.1　达标训练题

1.　__(1)__是计算机系统之间通信的层次、各对等层的通信协议以及相邻层间接口的集合。__(2)__是计算机网络和分布式系统在相互通信的对等层实体间交换信息所必须遵守

的规则集合。__(3)__是研究如何设计和构造协议规范，以及如何将所设计和构造的协议规范快速、准确、低成本地转化为可执行代码的一门科学。当前，基于__(4)__协议栈的互联网体系结构是计算机网络体系结构的主流，该结构仍在不断的改进和发展中，以满足多媒体计算机通信业务的需要。__(5)__不是协议的关键成分。

(1) A. 网络拓扑结构　B. 协议工程　C. 网络协议　D. 网络体系结构

(2) A. 网络接口　B. 网络工程　C. 网络协议　D. 网络拓扑

(3) A. 网络服务　B. 协议工程　C. 网络工程　D. 网络测试

(4) A. TCP/IPX　B. TCP/IP　C. SPX/IP　D. SPX/IPX

(5) A. 分层　B. 语义　C. 定时　D. 语法

2. 下列说法中正确的是________。

A. OSI 的网络层负责路由数据通过网络的功能

B. OSI 的会话层提供交互会话的管理功能，它控制数据流的方向，包括不多于两路的同步通话

C. OSI 的数据链路层在系统之间提供可靠的透明的数据传送，提供链路传输的流量的控制和错误恢复等功能

D. OSI 的表示层代表应用层进程协商数据表示，完成数据交换、数据格式化和数据压缩等功能

3. 下列关于面向连接和无连接的数据传输速度的说法中，正确的是________。

A. 面向连接的网络数据传输速度快

B. 面向无连接的网络数据传输速度快

C. 两者速度一样快

D. 不好判断它们的速度到底谁快

4. 物理层接口中信号线的工作规则和先后顺序是物理层接口中________定义的。

A. 机械特性　B. 电气特性　C. 功能特性　D. 规程特性

5. 典型的网络拓扑结构可以分为星型、__(1)__、总线型、树型。其中，星型结构的主要特点是__(2)__，总线型结构的主要特点是__(3)__。

(1) A. 环型　B. 主从型　C. 混合型　D. 单一型

(2) A. 主从式网络　B. 平等式网络　C. 成本高　D. 可靠性好

(3) A. 主从式网络　B. 平等式网络　C. 适用于实时环境　D. 可靠性差

6. 传输层提供________服务。

A. 点到点通信　B. 端到端通信

C. 子网到子网通信　D. 网端到网端通信

7. 下面的说法不正确的是________。

A. 当物理线路连接成功时，就自然建立了一条物理连接

B. RS-232C 规定的是物理层的特性

C. 多路连接由传输层管理

D. 路由选择可以由数据链路层来完成

1.8.2 参考答案

1. (1) D　(2) C　(3) B　(4) B　(5) A
2. B
3. D
4. D
5. (1) A　(2) A　(3) B
6. A
7. D

第 2 章　数据通信基础

大纲要求：

- 信道特性。
- 调制和编码，包括 ASK、FSK、PSK、QPSK、抽样定理、PCM、编码。
- 传输技术，包括通信方式(单工/半双工/全双工、串行/并行)、差错控制、同步控制、多路复用。
- 传输介质，包括有线介质和无线介质。
- 线路连接设备，包括调制解调器、DSU 和 DCU。
- 物理层。

2.1　数据通信的基本概念

2.1.1　考点辅导

通信系统模型如图 2-1 所示。

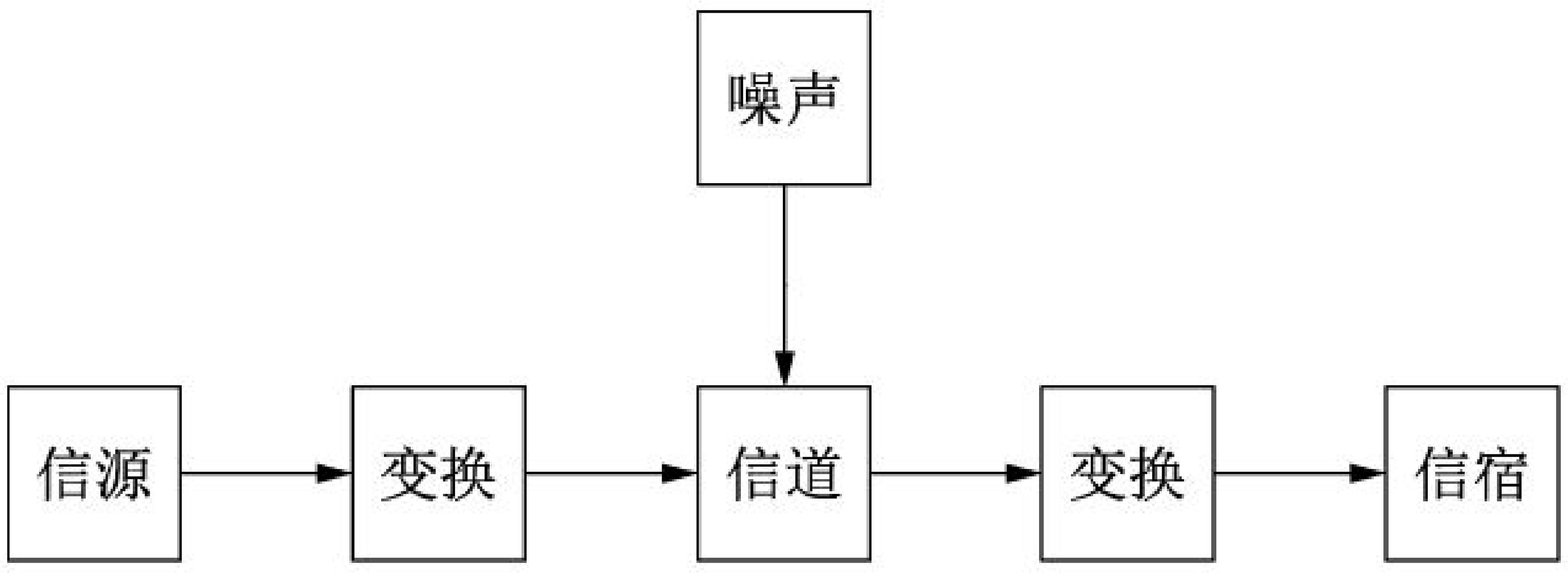


图 2-1　通信系统模型

通信中产生和发送信息的一端叫作信源，接收信息的一端叫作信宿，信源和信宿之间的通信线路称为信道。

模拟信号是随时间连续变化的信号，这种信号的某种参量(如幅度、相位、频率等)可以表示要传送的信息。

数字信号只取有限个离散值，而且数字信号之间的转换几乎是瞬时的。数字信号以某一瞬间的状态表示它们传送的信息。

如果信源产生的是模拟数据并以模拟信道传输，则称为模拟通信；如果信源发出的是模拟数据而以数字信号的形式传输，那么这种通信方式称为数字通信。

如果信源发出的是数字数据，当然也可以有两种传输方式，这时无论是用模拟信号传输还是用数字信号传输，都称为数据通信。可见，数据通信是专指信源和信宿中数据的形式是数字的，在信道中传输时则可以根据需要采用模拟传输方式或数字传输方式。

根据通信信号的传输方式，可以分为模拟传输和数字传输。

1. 模拟传输及其优、缺点

在模拟传输方式中，数据进入信道之前要经过调制，变换为模拟的调制信号。

优点：由于调制信号的频谱较窄，因此信道的利用率较高。

缺点：模拟信号在传输过程中会衰减，还会受到噪声的干扰，如果用放大器将信号放大，混入的噪声也会被放大。

2. 数字传输及其优、缺点

在数字传输方式中，可以直接传输二进制数据或经过二进制编码的数据，也可以传输数字化的模拟信号。

优点：由于数字信号只取有限个离散值，在传输过程中即使受到噪声的干扰，只要没有畸变到不可辨认的程度，就可以用信号再生的方法进行恢复，对某些数码的差错也可以用差错控制技术加以消除。另外，数字设备可以大规模集成，比复杂的模拟设备便宜得多。

缺点：传输数字信号比传输模拟信号所要求的频带要宽得多，因而信道利用率较低。

2.1.2　典型例题分析

例 2-1　5 个 64kb/s 的信道按统计时分多路复用在一条主线路上传输，主线路的开销为 4%，假定每个子信道利用率为 90%，那么这些信道在主线路上占用的带宽为<u>　(17)　</u>kb/s。(2017 年下半年真题 17)

A. 128　　B. 248　　C. 300　　D. 320

解析：每个子信道利用率为 90%，因此有此公式：$5\times64\times90\%=X\times(1-4\%)$，解方程得 $X=300$。其中 $5\times64\times90\%=288$kbps 为复用后的速率。

答案：C

例 2-2　如果信源产生的是模拟数据并以模拟信道传输，则叫作<u>　(1)　</u>；如果信源发出的是模拟数据而以数字信号的形式传输，那么这种通信方式叫作<u>　(2)　</u>。

(1)、(2)　A. 模拟通信　　B. 模拟数据

C. 数字通信　　D. 数据通信

解析：如果信源产生的是模拟数据并以模拟信道传输，则叫作模拟通信；如果信源发出的是模拟数据而以数字信号的形式传输，那么这种通信方式叫作数字通信。

答案：(1) A　(2) C

例 2-3　根据通信信号的传输方式，可以分为<u>　(1)　</u>、<u>　(2)　</u>。

(1)　A. 模拟传输　　B. 模拟信号　　C. 模拟信道　　D. 模拟通信

(2)　A. 数据通信　　B. 数字信道　　C. 数字传输　　D. 数字信号

解析：根据通信信号的传输方式，可以分为模拟传输、数字传输。在模拟传输方式中，数据进入信道之前要经过调制，变换为模拟的调制信号。在数字传输方式中，可以直接传输二进制数据或经过二进制编码的数据，也可以传输数字化的模拟信号。

答案：(1) A　(2) C

2.1.3 同步练习

1. 8 个 9600b/s 的信道按时分多路复用在一条线路上传输，在统计 TDM 情况下，假定每个子信道有 80%的时间忙，复用线路的控制开销为 5%，那么复用线路的带宽为______。

A. 32kb/s　　B. 64kb/s　　C. 72kb/s　　D. 96kb/s

2. 8 个 128kb/s 的信道通过统计时分复用到一条主干线路上，如果该线路的利用率为 90%，则其带宽应该是______kb/s。

A. 922　　B. 1024　　C. 1138　　D. 2276

3. CDMA 系统中使用的多路复用技术是______。

A. 时分多路　　B. 波分多路　　C. 码分多址　　D. 空分多址

4. 通常情况下，信息插座的安装位置距离地面的高度为______cm。

A. 10～20　　B. 20～30　　C. 30～50　　D. 50～70

5. 10 个 8.6kb/s 的信道按时分多路复用在一条线路上传输，如果忽略控制开销，在同步 TDM 情况下，复用线路的带宽应该是__(1)__；在统计 TDM 情况下，假定每个子信道有 30%的时间忙，复用线路的控制开销为 10%，那么复用线路的带宽应该是__(2)__。

(1)、(2) A. 32kb/s　　B. 64kb/s　　C. 72kb/s　　D. 96kb/s

A. 32kb/s　　B. 64kb/s　　C. 72kb/s　　D. 96kb/s

2.1.4 同步练习参考答案

1. B　　2. C　　3. C　　4. C　　5. (1) D　(2) A

2.2 信 道 特 性

2.2.1 考点辅导

2.2.1.1 信道带宽

1. 模拟信道带宽

模拟信道的带宽如图 2-2 所示。信道带宽 $W=f_2-f_1$，其中，f_1 是信道能通过的最低频率，f_2 是信道能通过的最高频率，两者都是由信道的物理特征决定的。为了使信号传输中的失真小些，信道要有足够的带宽。

2. 码元、波特率、数据速率、数字信道带宽

一个数字脉冲称为一个码元，用码元速率表示单位时间内信号波形的变换次数，即单位时间内通过信道传输的码元个数。若信号码元宽度为 T 秒，则码元速率 $B=1/T$，其单位为波特(baud)，码元速率也称波特率。若一无噪声信道的带宽为 W，则该信道的极限波特率为 $B=2W$ (奈奎斯特定理)。码元携带的信息量 n (比特)与码元的种类数 N 的关系为 $n=\log_2 N$。

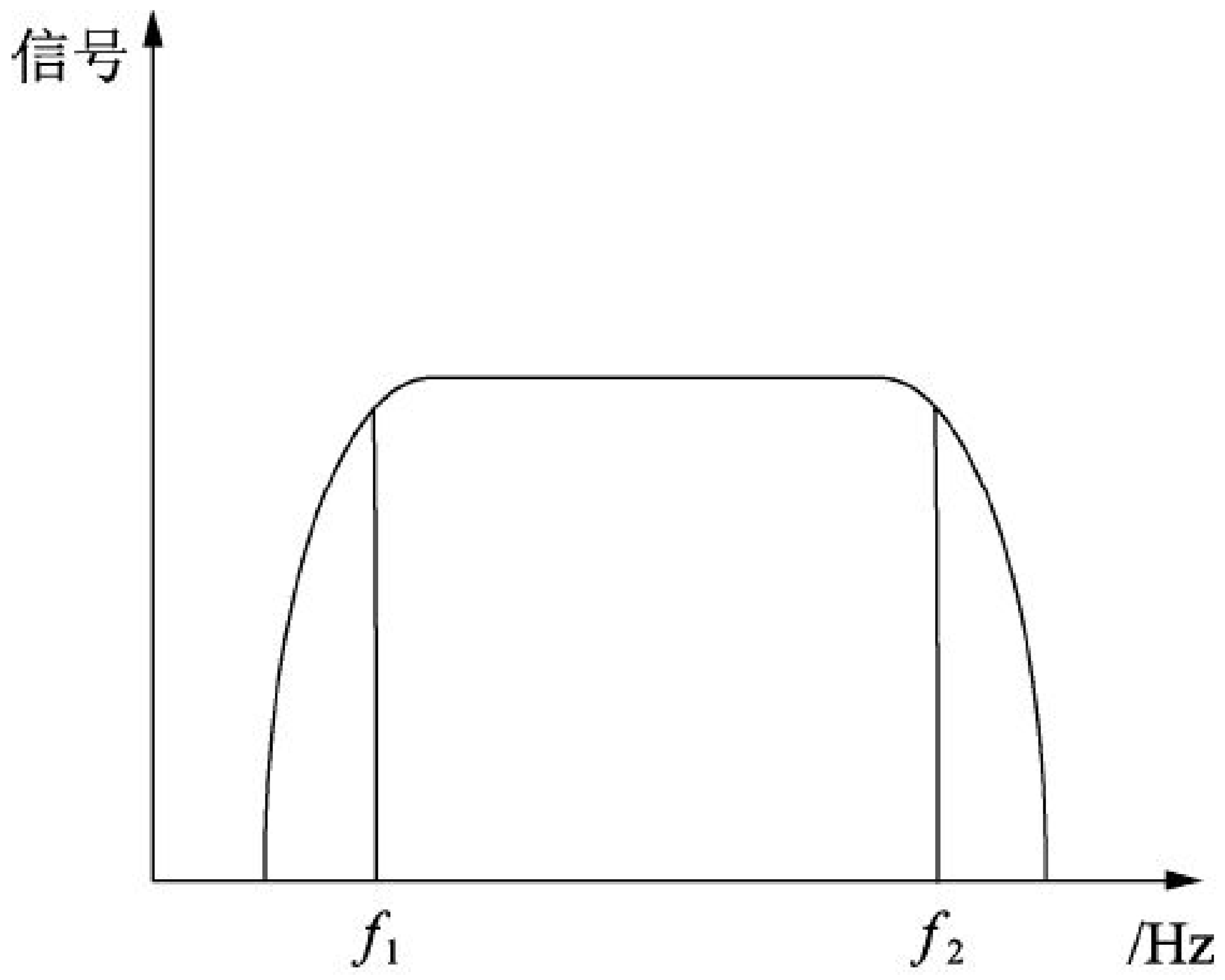


图 2-2　模拟信道的带宽

单位时间内在信道上传送的信息量(比特数)称为数据速率，其单位为比特。数据速率也称比特率。无噪声信道的极限数据速率为

$$R = B\log_2 N = 2W\log_2 N$$

式中：W 为信道带宽。

有噪声的极限数据速率为

$$C = W\log_2\left(1+\frac{S}{N}\right) \qquad \text{(香农定理)}$$

式中：W 为信道带宽；S 为信号的平均功率；N 为噪声平均功率；S/N 为信噪比。

数字信道的带宽为信道能够达到的最大数据速率。数字信道的带宽和模拟信道的带宽可以通过香农定理互相转换。

2.2.1.2　误码率、信道延迟

误码率表示传输二进制位时出现差错的概率，公式为 $P_c = N_e / N$，其中，N_e 为出错的位数，N 为传送的总位数。计算机通信一般要求误码率低于 10^{-6} (即平均 1 兆位错 1 位)。

信号在信道中传输，从源端到达宿端需要的时间称为信道延迟。网络不同，信道延迟对该网络应用产生的影响也不同。

2.2.2　典型例题分析

例 2-4　电话信道的频率为 0～4kHz，若信噪比为 30dB，则信道容量为__(12)__kb/s；要达到此容量，至少需要__(13)__个信号状态。(2017 年上半年真题 12、13)

(12) A.4　　B.20　　C.40　　D.80

(13) A.4　　B.8　　C.16　　D.32

解析：W(带宽)=4−0=4，由题可知 dB=$10\log_{10}(S/N)$=30，故 S/N=1000。

C(信道容量)=$W\times\log_2(1+S/N)=4\times\log_2 1001 \approx 4\times\log_2 2^{10}=40$。

$C=B\log_2 N=40$，又 $B=2W=8$。所以 $N=32$。

答案：(12) C　　(13) D

例 2-5　A、B 是局域网上两个相距 1km 的站点，A 采用同步传输方式以 1Mb/s 的速率

向 B 发送长度为 200 000 字节的文件。假定数据帧长为 128 比特，其中首部为 48 比特，应答帧为 22 比特，A 在收到 B 的应答帧后发送下一帧。传送文件花费的时间为__(15)__s，有效的数据速率为__(16)__Mb/s(传播速率为 200m/μs)。(2017 年上半年真题 15、16)

(15) A. 1.6　　B. 2.4　　C. 3.2　　D. 3.6

(16) A. 0.2　　B. 0.5　　C. 0.7　　D. 0.8

解析：总时间=传播时间+传输时间

发送 200 000 字节，需要发送数据帧=(20 0000×8)/(128−48)=20 000 个(数据帧)，那么应答帧=20 000 个。

传播时间=(1000/200)μs×40 000=0.2s

传输时间=发送数据帧时间+发送应答帧时间

发送一个数据帧时间：128/1 000 000s

发送一个应答帧时间：22/1 000 000s

所以，传输时间(150/1 000 000)×20 000=3s，则总时间=3.2s。

有效数据速率=(200 000×8)b/3.2s=0.5Mb/s。

答案：(15) C　　(16) B

例 2-6　电话线路使用的带通滤波器的带宽为 3kHz(即 300～3300Hz)，根据奈奎斯特采样定理，最小采样频率应为__(15)__。(2015 年上半年真题 15)

A. 300Hz　　B. 3390Hz　　C. 6000Hz　　D. 6600Hz

解析：根据奈奎斯特采样定理，采样频率至少为最高频率的 2 倍。

答案：D

2.2.3　同步练习

1. 设信道带宽为 4000Hz，信噪比为 30dB，按照香农定理，信道容量为______。

A. 4kb/s　　B. 1.6kb/s　　C. 40kb/s　　D. 120kb/s

2. 地面上相距 2000km 的两地之间通过电缆传输 4000 比特长的数据包，数据传输速率为 64kb/s，从开始发送到接收完成需要的时间为______。

A. 48ms　　B. 640ms　　C. 32.5ms　　D. 72.5ms

2.2.4　同步练习参考答案

1. C　　2. D

2.3　传 输 介 质

2.3.1　考点辅导

1. 双绞线

双绞线由粗约 1mm 的相互绝缘的一对铜导线绞扭在一起组成，对称均匀地绞扭可以减少线对之间的电磁干扰。双绞线大量使用在传统的电话系统中。双绞线分为屏蔽双绞线和非屏蔽双绞线。

2. 同轴电缆

同轴电缆的芯线是铜质导线，外包一层绝缘材料，再外面是由细铜丝组成的网状导体，最外面加一层塑料保护膜，具有高带宽和较好的噪声抑制特性。局域网中常用的同轴电缆有两种：一种是特性阻抗为 50Ω，用于传输数字信号，叫作基带同轴电缆；另一种是特性阻抗为 75Ω 的 CATV 电缆，用于传输模拟信号，叫作宽带同轴电缆。

3. 光缆

光缆由能传送光波的超细玻璃纤维(即光纤)和其他材料组合而成，光纤外包一层比玻璃折射率低的材料。进入光纤的光波在两种材料的界面上形成全反射，从而不断地向前传播。光纤分为多模光纤和单模光纤两种。在多模光纤中，光波以多种模式传播，不同的传播模式有不同的电磁场分布和不同的传播路径。在单模光纤中，光在其中无反射地沿直线传播。光纤的优点是具有很高的数据速率、极宽的频带、低误码率和低延迟，而且安全性和保密性好。

4. 无线信道

无线信道包括微波、红外和短波信道。

微波通信系统可分为地面微波系统和卫星微波系统。微波通信的频段一般是 1～11GHz，具有带宽高、容量大、天线小、便于安装和移动的优点；缺点是容易受到电磁干扰，微波通信相互间也存在干扰，微波信号容易被大气层中的雨雪吸收。另外，在卫星微波系统中，信号时延也比较大。

红外传输系统利用墙壁或屋顶反射红外线，从而形成整个房间内的广播通信系统。优点是设备相对便宜，带宽高；缺点是传输距离有限，且易受室内空气状态的影响。

无线电短波通信使用甚高频和超高频的电视广播频段。优点是通信设备比较便宜，便于移动，没有方向性；缺点是容易受到电磁干扰和地形地貌的影响，而且带宽比微波通信小。

2.3.2　典型例题分析

例 2-7　100Base-T4 采用的编码技术为__(14)__，利用__(15)__传输介质进行数据传输。(2017 年下半年真题 14、15)

(14) A. 4B/5B　　B. 8B/6T　　C. 8B/10B　　D. MTL-3

(15) A. 光纤　　B. UTP-5　　C. UTP-3　　D. 同轴电缆

解析：100Base-T4 的信号采用 8B/6T 的编码方式，即每 8 位作为一组的数据转换为每 6 位一组的三元码组。其电缆类型为 4 对三类非屏蔽双绞线，最大传送距离是 100 米。

答案：(14)　B　　(15)　C

2.3.3　同步练习

1.　以下关于光纤通信的叙述中，正确的是______。

A. 多模光纤传输距离远，单模光纤传输距离近
B. 多模光纤的价格便宜，单模光纤的价格较贵
C. 多模光纤的包层外径较粗，单模光纤的包层外径较细
D. 多模光纤的纤芯较细，单模光纤的纤芯较粗

2. 光纤分为单模光纤和多模光纤，这两种光纤的区别是______。
A. 单模光纤的数据速率比多模光纤低　B. 多模光纤比单模光纤传输距离更远
C. 单模光纤比多模光纤的价格更便宜　D. 多模光纤比单模光纤的纤芯直径粗

3. 光纤分为单模光纤和多模光纤，这两种光纤的区别是______。
A. 单模光纤的纤芯大，多模光纤的纤芯小
B. 单模光纤比多模光纤采用的波长长
C. 单模光纤的传输频带窄，多模光纤的传输频带宽
D. 单模光纤的光源采用发光二极管(Light Emitting Diode，LED)，多模光纤的光源采用激光二极管(Laser Diode，LD)

2.3.4 同步练习参考答案

1. B　2. D　3.B

2.4 数 据 编 码

2.4.1 考点辅导

数据编码的方式很多，主要有以下几种(见图 2-3)。

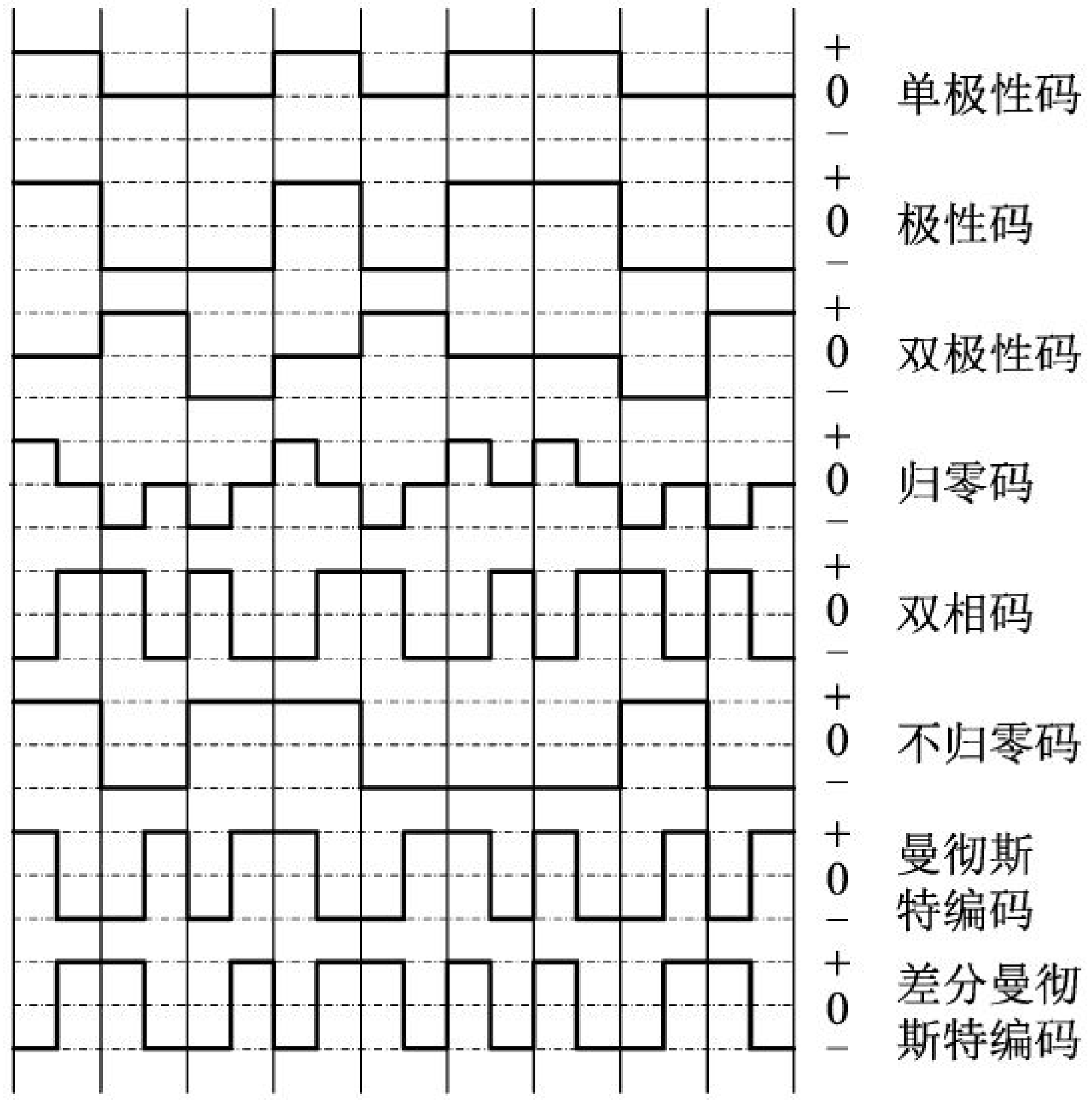


图 2-3　常用编码方案

1. 单极性码

在单极性码这种编码方案中，只用正的(或负的)电压表示数据。在图 2-3 中，用+3V 表示二进制数字 0，用 0V 表示二进制数字 1。单极性码用在电传打字机(TTY)接口以及 PC 和 TTY 兼容的接口中，这种代码需要单独的时钟信号配合定时，它的抗噪声特性也不好。

2. 极性码

在极性码这种编码方案中，分别用正和负电压表示二进制数 0 和 1。例如，在图 2-3 中用+3V 表示二进制数字 0，而用−3V 表示二进制数字 1。这种代码抗干扰特性好，但仍然需要另外的时钟信号。

3. 双极性码

在双极性码这种编码方案中，信号在 3 个电平(正、负、零)之间变化。一种典型的双极性码是信号交替反转编码(AMI)。在 AMI 信号中，数据流中遇到 1 时，电平在正和负之间交替翻转；遇到 0 时，则保持零电平。双极性码是三进制信号编码方法，与二进制相比抗噪声特性更好。

4. 归零码

在归零码中，码元中间的信号回归到 0 电平，因此任意两个码元之间被 0 电平隔开。这种编码方案有较好的噪声抑制特性。图 2-3 表示的是一种双极性归零码。可以看出，从正电平到零电平的转换边表示码元 0，从负电平到零电平的转换边表示码元 1，同时每一位码元中间都有电平转换，使得这种编码成为自定时的编码。

5. 双相码

双相码要求每一位中都要有一个电平转换。这种代码是自定时的，同时也有检测错误的功能；如果某一位中间缺少了电平翻转，则被认为是错误代码。

6. 不归零码

图 2-3 所示的不归零码的规律是：当 1 出现时电平翻转，当 0 出现时电平不翻转。因而区别 1 和 0 的是电平是否翻转。这种代码也叫差分码，用在终端到调制解调器的接口中。这种代码不是自定时的。

7. 曼彻斯特编码

曼彻斯特编码是一种双相码。图 2-3 中，用高电平到低电平的转换边表示 0；用低电平到高电平的转换边表示 1；位中间的电平转换边既表示数据代码，也作为定时信号使用。这种编码用在以太网中。

8. 差分曼彻斯特编码

差分曼彻斯特编码也是一种双相码。这种编码码元中间的电平转换边只作为定时信号，不表示数据。数据的表示在于每一位开始处是否有电平转换：有电平转换表示 0；无电平转换表示 1。这种编码用在令牌环网中。

9. 多电平编码

多电平编码的码元可取多个电平之一，每个码元可代表几个二进制位。例如，若表示

码元的脉冲取四个电平之一，则一个码元可表示两个二进制位。

10. 4B/5B 编码

4B/5B 编码是将欲发送的数据流每 4 位作为一个组，然后按照编码规则将其转换成相应的 5 位码。该编码属于自同步编码方式，为了保证接收端能提取同步时钟，编码规则保证：无论 4 位数据为何种组合(包括全部为 0)，所转换成 5 位码中，至少有两个“1”，即保证在传输过程中码元至少发生两跳变，从而保证接收端同步时钟的提取。4B/5B 编码能较好地解决同步问题，同时具有检错功能，编码效率比较高，它用 5 位信号表示 4 位有效信息，因此编码效率为 80%。若要达到 100Mb/s 的速率，只需在线路上有 125Mbaud 的波特率。快速以太网(100Base-T)和光纤分布式接口(FDDI)都采用 4B/5B 编码方式。

2.4.2 典型例题分析

例 2-8 4B/5B 编码先将数据按 4 位分组，将每个分组映射到 5 单位的代码，然后采用 (14) 进行编码。(2017 年上半年真题 14)

A. PCM　　B. Manchester　　C. QAM　　D. NRZ-I

解析：4B/5B 编码实际上是一种两级编码。系统中使用不归零编码，在发送到传输介质之前要变成见 1 就翻的不归零编码(NRZ-I)。NRZ-I 代码序列中 1 的个数越多，越能提供同步定时信息，但如果遇到长串的 0，则不能提供同步信息。所以在发送到介质之前还需要进行一次 4B/5B 编码，发送器扫描要发送的位序列，将其每 4 位分成一组，然后按照 4B/5B 编码规则转换成相应的 5 位代码。

答案：D

2.4.3 同步练习

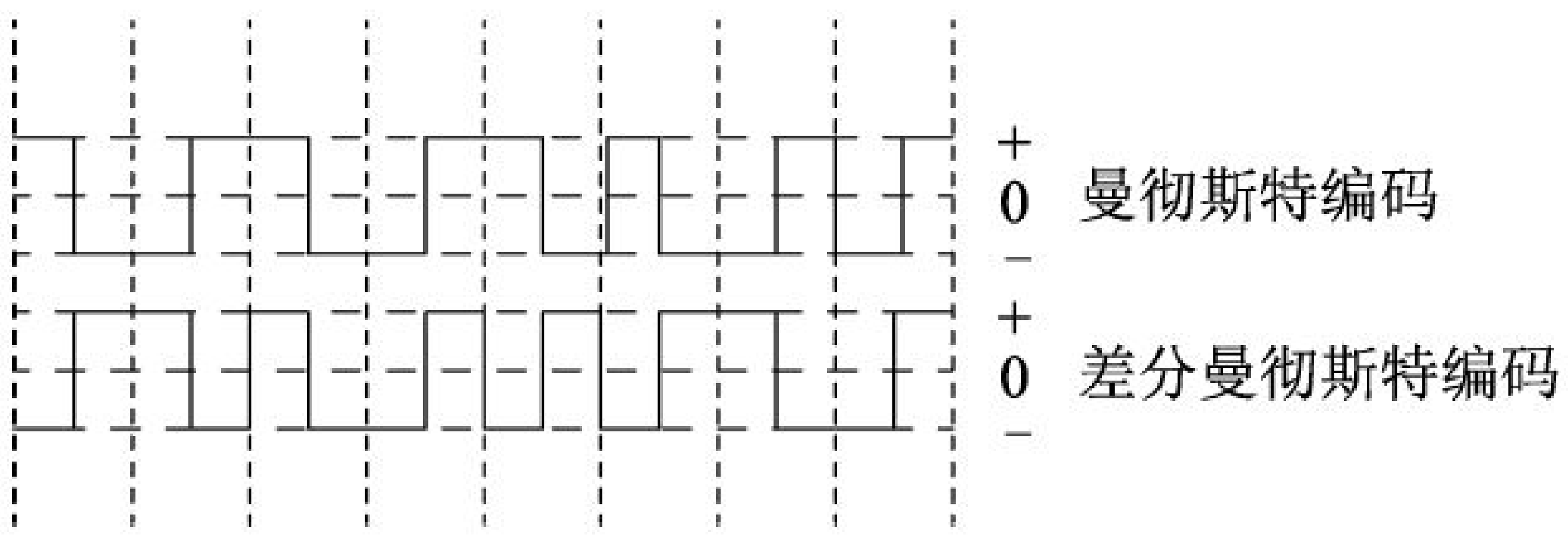
1. 曼彻斯特编码的效率是 (1) %，4B/5B 编码的效率是 (2) %。

(1)、(2) A. 40　　B. 50　　C. 80　　D. 100

2. 10Base-T 以太网使用曼彻斯特编码，其编码效率为 (1) %；在快速以太网中使用 4B/5B 编码，其编码效率为 (2) %。

(1)、(2) A. 30　　B. 50　　C. 80　　D. 90

3. 下图为曼彻斯特编码和差分曼彻斯特编码的波形图，实际传送的比特串为____。



A. 1 0 1 0 1 1 0 0　　B. 0 1 1 1 0 0 1 0

C. 0 1 0 1 0 0 1 1　　D. 1 0 0 0 1 1 0 1

2.4.4　同步练习参考答案

1. (1) B　(2) C

2. (1) B　(2) C　　　3. C

2.5　数字调制技术

2.5.1　考点辅导

数字数据在传输中不仅可以用方波脉冲表示，也可以用模拟信号表示。数字调制指用数字数据调制模拟信号。主要有 3 种基本的调制方法，即调幅、调频、调相。

1. 调幅

调幅(也称幅度键控，ASK)，是指将不同的数据信息 1 和 0 调制成不同幅度但相同频率的载波信号。

2. 调频

调频(也称频移键控，FSK)，是指将不同的数据信息 1 和 0 调制成相同幅度但不同频率的载波信号。

3. 调相

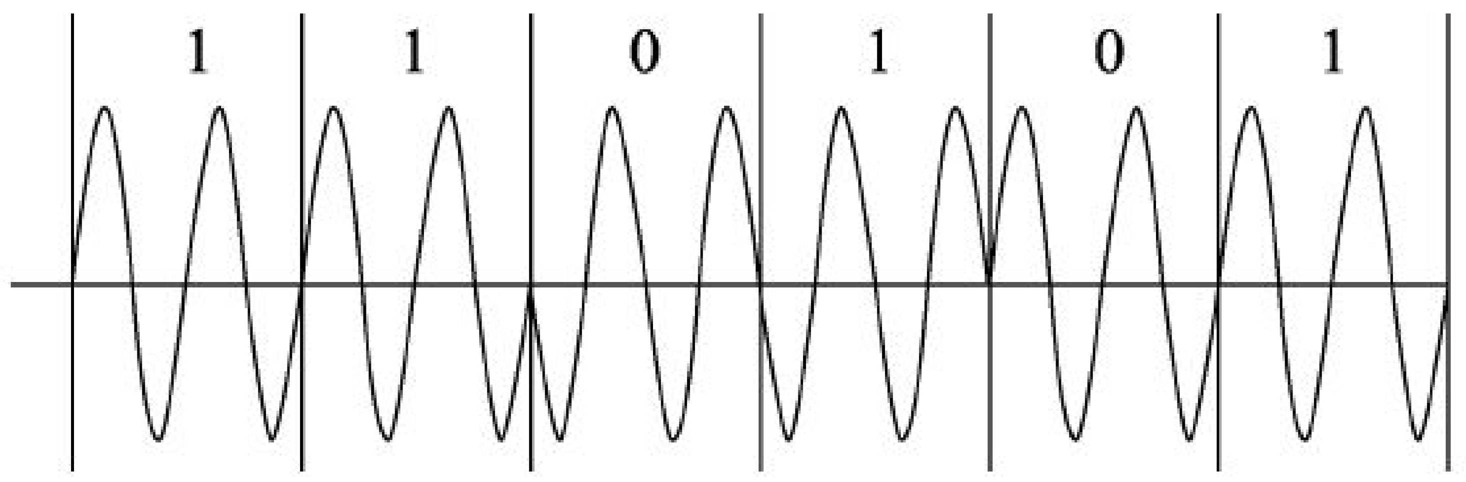
调相(也称相移键控，PSK)，是指利用相邻载波信号的相位变化值来表示相邻信号是否具有相同的数据信息值，此时的幅度和频率均保持不变。

4. 正交调幅

正交调幅(QAM)是一种十分成熟且应用广泛的调制技术。其基本方法是将发送数据流分为两路，分别对正弦载波和余弦载波进行数字调幅，然后相加传输。如果每路载波有 n 个不同幅度，则 QAM 信号的星座图上有 n^2 个状态点。这种方式的频谱利用率可以做得很高，设备也不太复杂。但是，当它的信号状态数很多时，会对信道的线性和非线性失真变得十分敏感，需要采用多种措施来对抗。

2.5.2　典型例题分析

例 2-9　下图所示的调制方式是__(11)__，若数据速率为 1kb/s，则载波速率为__(12)__ Hz。(2017 年下半年真题 11、12)



(11) A. DPSK　　B. BPSK　　C. QPSK　　D. MPSK

(12) A. 1000　　B. 2000　　C. 4000　　D. 8000

解析：根据图形可知波形在 1 和 0 之间，以载波的相对初始相位变化来实现数据的传送，并且初始相位与前一码元发生 180° 变化为二进制 0，无变化为 1，可以判定为 DPSK(差分相移键控)。对应的码元速率和二进制数据速率相同，数据速率为 1Kb/s，因此载波频率为两倍。

答案：(11) A　(12) B

例 2-10　通过正交幅度调制技术把 ASK 和 PSK 两种调制模式结合起来组成 16 种不同的码元，这时数据速率是码元速率的__(14)__倍。(2016 年上半年真题 14)

A. 2　B. 4　C. 8　D. 16

解析：所谓正交幅度调制(Quadrature Amplitude Modulation，QAM)，就是把两个幅度相同但相位相差 90° 的模拟信号合成为一个模拟信号。通过把 ASK 和 PSK 技术结合起来，形成幅度相位复合调制，这也是一种正交幅度调制技术。由于形成了 16 种不同的码元，所以每一个码元可以表示 4 位二进制数据，即数据速率为码元速率的 4 倍，使得数据速率大大提高。

答案：B

例 2-11　设信号的波特率为 500Baud，采用幅度-相位复合调制技术，由 4 种幅度和 8 种相位组成 16 种码元，则信道的数据速率为__(15)__。(2015 年下半年真题 15)

A. 500b/s　B. 1000b/s　C. 2000b/s　D. 4800b/s

解析：数据传输速率 R 与波特率 B 之间的换算公式为 $R = B\log_2 N$。N 为码元的种类，本题为 16，因此 $R = 500\times\log_2 16 = 500\times 4 = 2000$ b/s。

答案：C

例 2-12　正交幅度调制 16-QAM 的数据速率是码元速率的__(14)__倍。(2015 年上半年真题 14)

A. 2　B. 4　C. 8　D. 16

解析：正交幅度调制形成了 16 种不同的码元，数据传输速率 R、码元速率 B、码元种类之间的关系是 R=$B\log_2N$，因此 R=$B\log_2 16$=4B，可见数据速率是码元速率的 4 倍。

答案：B

2.5.3　同步练习

所谓正交幅度调制是把两个______的模拟信号合为一个载波信号。

A. 幅度相同，相位相差 90°　B. 幅度相同，相位相差 180°
C. 频率相同，相位相差 90°　D. 频率相同，相位相差 180°

2.5.4　同步练习参考答案

A

2.6　脉冲编码调制

2.6.1　考点辅导

脉冲编码调制(PCM)是一种数字化技术，用于将模拟数据变换为数字信号。变换的过程分为 3 个步骤，即采样、量化和编码。

1. 采样

采样是指每隔一定时间间隔，取模拟信号的当前值作为样本，该样本代表了模拟信号在某一时刻的瞬时值。这样，就变连续的模拟信息为离散信号。采样技术依据奈奎斯特取样定理：如果采样速率大于模拟信号最高频率的 2 倍，则可以用得到的样本空间恢复原来的模拟信号。

2. 量化

量化的目的是确定采样出的模拟信号的数值。通过规定一定的量化级，对采样得到的模拟信号数值进行“取整”量化，得到离散信号的具体数值。量化级越高，表示离散信号的值精度越高。

3. 编码

编码是指将量化后的样本值变成相应的二进制代码。通常，当量化级为 N 时，二进制位数为 $\log_2 N$。

例如，对声音数字化时，由于话音的最高频率是 4kHz，所以采样速率是 8kHz。对话音样本的量化用 128 个等级，因而每个样本用 7 位二进制数字表示。在数字信道上传输的速率是 7×8000=56kb/s。

2.6.2　典型例题分析

例 2-13　数字语音的采样频率定义为 8kHz，这是因为__(6)__。(2017 年上半年真题 6)

A. 语音信号定义的频率最高值为 4kHz

B. 语音信号定义的频率最高值为 8kHz

C. 数字语音传输线路的带宽只有 8kHz

D. 一般声卡的采样频率最高为每秒 8kHz

解析：本题考查奈奎斯特取样定理：如果取样速率大于模拟信号最高频率的 2 倍，则可以用得到的样本恢复原来的模拟信号。因此采样频率=模拟信号频率×2，即模拟信号频率为 4kHz。

答案：A

2.6.3 同步练习

1. 假设模拟信号的最高频率为 10MHz，采样频率必须大于______时，才能使得到的样本信号不失真。

A. 6MHz　　B. 12MHz　　C. 18MHz　　D. 20MHz

2. 假设模拟信号的最高频率为 6MHz，采样频率必须大于______时，才能使得到的样本信号不失真。

A. 6MHz　　B. 12MHz　　C. 18MHz　　D. 20MHz

3. 设信道带宽为 3400Hz，采用 PCM 编码，采样周期为 125μs，每个样本量化为 128 个等级，则信道的数据速率为______。

A. 10kb/s　　B. 16kb/s　　C. 56kb/s　　D. 64kb/s

4. 假设模拟信号的最高频率为 5MHz，采样频率必须大于 (1) ，才能使得到的样本信号不失真；如果每个样本量化为 256 个等级，则传输的数据频率是 (2) 。

(1) A. 5MHz　　B. 10MHz　　C. 15MHz　　D. 20MHz

(2) A. 10Mb/s　　B. 50Mb/s　　C. 80Mb/s　　D. 100Mb/s

2.6.4 同步练习参考答案

1. D　　2. B　　3. C　　4. (1) B　(2) C

2.7 通信方式和交换方式

2.7.1 考点辅导

2.7.1.1 数据通信方式

1. 按通信方向分类

按数据传输的方向分类，有 3 种不同的通信方式，即单工、半双工和全双工。

1) 单工

单工方式下，信道上的信息只能向一个方向传送，发送方不能接收，接收方也不能发送。如无线电广播和电视广播。

2) 半双工

半双工方式下，通信的双方可交替发送和接收信息，但不能同时发送和接收。在一段时间内，信道的全部带宽用于向一个方向上传送信息，如对讲机通信。

3) 全双工

全双工方式下，可同时进行双向信息的传送，要求通信双方都有发送和接收设备，如电话通信。

2. 按同步方式分类

在传送由多个码元组成的字符以及由许多字符组成的数据块时，通信双方要就信息的起止时间取得一致。有两种不同的传输方式，即同步传输和异步传输。

1) 同步传输

同步传输适合传输连续的数据块。在这种方式下，发送方在发送数据前先发送一串同步字符 SYNC。接收方只要检测到连续两个以上 SYNC 字符就确认已进入同步状态，准备接收信息。随后的传送过程中双方以同一频率工作(信号编码的定时作用也表现在这里)，直到传送完指示数据结束的控制字符。

2) 异步传输

异步传输即把各个字符分开传输，字符之间插入同步信息。这种方式也称起止式，即在字符的前后分别插入起始位(“0”)和停止位(“1”)。起始位对接收方的时钟起置位作用。停止位告诉接收方该字符传送结束，然后接收方就可以检测后续字符的起始位。当没有字符传送时，连续传送停止位。

2.7.1.2　信息交换方式

通信网络由许多交换节点互联而成，交换节点转发信息的方式可分为电路交换、报文交换和分组交换等。

1. 电路交换

电路交换交换方式把发送方和接收方用物理线路直接连通。类似于电话系统，此方式下的数据通信希望通信的计算机之间必须事先建立物理线路。整个电路交换的过程包括建立线路、数据传输、释放线路 3 个阶段。

(1) 建立线路。发送方向接收方发送一个请求，该请求通过中间节点传输至终点；如果中间节点有空闲的物理线路可用，则接受请求，分配线路，并将请求传输给下一个中间节点。整个过程持续进行，直至终点。线路一旦被分配，在未释放之前，其他站点将无法使用。

(2) 数据传输。在已经建立的物理线路上，发送方和接收方进行数据传输。

(3) 释放线路。当数据传输完毕，执行释放线路的动作。线路被释放之后，进入空闲状态，可供其他站点通信使用。

电路交换的优点是独占性、实时性好，适合传输大量的数据。

2. 报文交换

报文交换也称存储—转发交换。这种方式不要求在两个通信节点之间建立专用线路。节点把要发送的信息组织成一个数据包——报文，该报文中含有目标节点的地址，完整的报文在网络中一站一站地向前传送。每一个节点接收整个报文，检查目标节点地址，然后根据网络中的交通情况在适当的时候转发到下一个节点。经过多次的存储—转发，最后到达目标节点。其中的交换节点要有足够大的存储空间，用以缓冲收到的长报文。交换节点对各个方向上收到的报文排队，寻找下一个转发节点，然后再转发出去，这些都带来了排队等待延迟。

报文交换的优点是不建立专用线路，线路利用率较高；缺点是有通信时延。

3. 分组交换

分组交换技术类似报文交换，只是它规定了交换设备处理和传输的数据长度(称为分组)。通常，分组的长度远小于报文交换中规定的报文长度。进行分组交换时，发送节点先对传送的信息分组，对各个分组编号，加上源地址和目标地址以及约定的分组头信息。一次通信中的所有分组在网络中传播又有两种方式：数据报和虚电路。

1) 数据报

数据报类似于报文交换，每个分组都有完整的地址信息，不出意外的话都可以到达目的地。但是到达顺序可能与发送顺序不一致，因此目标主机必须对收到的分组重新排序。这就需要在发送端有分组拆装设备对信息进行分组和编号，而在接收端需要有分组拆装设备对收到的分组去头去尾并重新排序。数据报方式适合于单向地传送短消息。

2) 虚电路

虚电路类似于电路交换，要求在发送端和接收端之间建立一条逻辑连接。发送端发出的分组都走这一条通路，接收方要对正确收到的分组给予回答确认，直到会话结束，拆除连接。逻辑连接的建立不意味着别的通信不能使用这条线路，仍然可以共享。虚电路适合于交互式通信。

2.7.2 典型例题分析

例 2-14 在异步通信中，每个字符包含 1 位起始位、8 位数据位、1 位奇偶位和 2 位终止位，若有效数据速率为 800bp/s，采用 QPSK 调制，则码元速率为 (16) 波特。(2017 年下半年真题 16)

A. 600　　B. 800　　C. 1200　　D. 1600

解析：每个字符的位数为 1+8+1+2=12，有效数据速率=标准速率×8/12=800b/s，则可得标准速率是 1200b/s。采用 QPSK 调制，那么码元速率×$\log_2 4$=1200，可得出码元速率为 600 波特。

答案：A

例 2-15 在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 1 位终止位，每秒钟传送 100 个字符，采用 DPSK 调制，则码元速率为 (14) ，有效数据速率为 (15) 。(2016 年下半年真题 14、15)

(14) A. 200 波特　　B. 500 波特　　C. 1000 波特　　D. 2000 波特

(15) A. 200b/s　　B. 500b/s　　C. 700b/s　　D. 1000b/s

解析：DPSK(差分相移键控)利用调制信号前后码元之间载波相对相位的变化来传递信息。码元速率=(1+7+1+1) × 100=1000 波特，有效数据速率=[7/(1+7+1+1)] × 1000=700b/s。

答案：(14) C　(15) C

2.7.3 同步练习

1. 在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 2 位终止位，

每秒钟传送 100 个字符，则有效数据速率为________。

A. 100b/s　　B. 500b/s　　C. 700b/s　　D. 1000 b/s

2. 下列选项中，不采用虚电路通信的网络是________网。

A. X.25　　B. 帧中继　　C. ATM　　D. IP

3. 在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶校验位和 1 位终止位，每秒钟传送 200 个字符，采用 DPSK 调制，则码元速率为__(1)__，有效数据速率为__(2)__。

(1) A. 200 波特　　B. 500 波特　　C. 1000 波特　　D. 2000 波特

(2) A. 200b/s　　B. 1000b/s　　C. 1400b/s　　D. 2000b/s

2.7.4　同步练习参考答案

1. C　　2. D　　3. (1) D　(2) C

2.8　多路复用技术

2.8.1　考点辅导

1. 频分多路复用

频分多路复用(FDM)是在一条传输介质上使用多个频率不同的模拟载波信号进行多路传输。该技术对整个物理信道的可用带宽进行分割，利用载波调制技术实现原始信号的频谱迁移，使得多路信号在整个物理信道带宽允许的范围内，实现频谱上的不重叠，从而共用一个信道。为了防止相互干扰，子信道间留有一定宽度的隔离频带。

2. 时分多路复用

时分多路复用(TDM)用于数字信道的复用。当物理信道可支持的位传输速率超过单个原始信号要求的数据传输速率时，可以将该物理信道划分成若干个时间片，并将各个时间片轮流地分配给多路信号，使得它们在时间上不重叠。时间片的宽度可以容纳一位、一字节或一个固定大小的数据块。

3. 波分多路复用

波分多路复用(WDM)用于光纤通信中，不同的子信道用不同波长的光波承载，多路复用信道同时传送所有子信道的波长。因此要使用能够对光波进行分解和合成的多路器。

4. 码分多路复用

码分多路复用(CDMA)也叫码分多址，是一种扩频多址的数字通信技术。在 CDMA 系统中，每个移动站都有相互正交的一个码片(Chip)，当发送码片序列时表示 1，当发送码序列的反码时表示 0。典型的应用是目前流行的 3G 技术。

5. 数字传输系统

T1 载波在北美和日本广泛使用。它把 24 路按时分多路的原理复合在一条 1.544Mb/s 的高速信道上。每路话音信道有 7 位数据位和 1 位信令位，周期为 125μs，因此 24 路话音信道可容纳 8×24=192 位长的数字串。这 192 位数字组成一帧，最后再加入一个帧同步位，故帧长为 193 位。每 125μs 传送一帧，这样对每一路话音信道来说，传输数据的速率为 7b/125μs=56kb/s，传输控制信息的速率为 1b/125μs=8kb/s，总的速率为 193b/125μs=1.544Mb/s。

E1 载波在北美和日本以外的国家使用(欧洲标准)。国际电报电话咨询委员会(Commite' Consultatif International de Telegraphique et Telephonique，CCITT)于 1993 年后改为 ITU-T，建议了一种 PCM 传输标准，称为 E1 载波。该载波把一个时分复用帧(其长度 T=125μs)划分为 32 个相等的时隙，每个时隙 8 位，时隙的编号为 CH0～CH31，其中时隙 CH0 用作帧同步，时隙 CH16 用来传送信令，其他 30 时隙用作 30 个话路。E1 信道的传输速率为 8×32B÷125μs=2.048Mb/s。

E2 载波由 4 个 E1 载波组成，数据速率为 7.448Mb/s；E3 载波由 4 个 E2 载波组成，数据速率为 34.368Mb/s；E4 载波由 4 个 E3 载波组成，数据速率为 138.24Mb/s；E5 载波由 4 个 E4 载波组成，数据速率为 565.148Mb/s。

6. 同步数字系列

光纤线路的多路复用标准有两个，即美国标准(SONET)和国际标准(SDH)。

SONET 的各级时钟都来自一个非常精确的主时钟。SONET 定义了同步传输的线路速率的等级结构，其传输速率以 51.840Mb/s 为基础。此速率对于电信号称为第一级同步传送信号，即 STS-1；对于光信号则称为第一级光载波，即 OC-1。

ITU-T 以美国标准 SONET 为基础，制定出国际标准同步数字系列 SDH。一般可认为 SDH 与 SONET 是同义词。SDH 的基本速率为 155.52Mb/s，称为第一级同步传递模块(Synchronous Transfer Module)，即 STM-1，相当于 SONET 体系中的 OC-3 速率。

2.8.2 典型例题分析

例 2-16 E1 载波的子信道速率为__(13)__kb/s。(2017 年下半年真题 13)

A. 8　　B. 16　　C. 32　　D. 64

解析： E1 载波的传输速率为 2.048Mb/s，每个子信道的速率是 64kb/s。

答案： D

例 2-17 T1 载波的数据速率是__(17)__。(2016 年上半年真题 17)

A. 1.544Mb/s　　B. 6.312Mb/s　　C. 2.048Mb/s　　D. 44.736Mb/s

解析： T1 载波也叫一次群，它把 24 路话音信道按时分多路的原理复合在一条高速信道上。该系统的工作是这样的，用一个编码解码器轮流对 24 路话音信道取样、量化和编码，一个取样周期中(125ms)得到的 7 位一组的数字组合成一串，共 7×24 位长。这样的数字串在送入高速信道前要在每一个 7 位组的后面插入一个信令位，于是变成了 8×24=192 位长的数字串。这 192 位数字组成一帧，最后再加入一个帧同步位，故帧长为 193 位。每 125μs 传

送一帧，其中包含了各路话音信道的一组数字，还包含总共 24 位的控制信息以及 1 位帧同步信息。这样，不难算出 T1 载波的各项比特率。对每一路话音信道来说，传输数据的比特率为 7b/125μs=56kb/s，传输控制信息的比特率为 1b/125μs=8kb/s，总的比特率为 193b/125μs=1.544Mb/s。

答案：A

2.8.3　同步练习

1.　E1 载波的数据速率是__(1)__Mb/s，T1 载波的数据速率是__(2)__Mb/s。

(1)、(2)　A. 1.544　　B. 2.048　　C. 6.312　　D. 7.448

2.　E1 信道的数据速率是__(1)__，其中每个话音信道的数据速率是__(2)__。

(1)　A. 1.544Mb/s　　B. 2.048Mb/s　　C. 6.312Mb/s　　D. 44.736Mb/s

(2)　A. 56kb/s　　B. 64kb/s　　C. 128kb/s　　D. 2048kb/s

2.8.4　同步练习参考答案

1. (1) B　(2) A　　　2. (1) B　(2) B

2.9　差 错 控 制

2.9.1　考点辅导

通信系统必须考虑如何发现和纠正信号传输中的差错。通信过程中出现的差错可大致分为两类：一类是由热噪声引起的随机错误；另一类是由冲击噪声引起的突发错误。下面介绍 3 种常用的差错控制技术。

1. 检错码

奇偶校验是最常用的检错方法。奇偶校验码包括水平奇偶校验码、垂直奇偶校验码和水平垂直奇偶校验码。

1)　水平奇偶校验码

水平奇偶校验码也称字符校验码，是在 7 位的 ASCII 代码后增加一位，使码字中“1”的个数成奇数(奇校验)或偶数(偶校验)；经过传输后，如果其中一位出错，则接收端按同样的规则就能发现错误。CCITT 规定，异步传输方式中采用偶校验，同步传输方式中采用奇校验。

2)　垂直奇偶校验码

垂直奇偶校验也称组校验，是指被传输的信息进行分组，并排列为若干行和列；组中每个字符的相同位进行奇偶校验，最终产生由校验位形成的校验字符，并附加在信息分组之后传输。

3) 水平垂直奇偶校验码

水平垂直奇偶校验也称方阵校验，是在水平校验的基础上实施垂直校验。此时，为了保证随后一位的正确填充，水平垂直奇偶校验应采用偶校验。

2. 海明码

1950 年，海明研究了用冗余数据位来检测和纠正代码差错的理论和方法。按照海明的理论，可以在数据代码上添加若干冗余位组成码字。码字之间的海明距离是一个码字要变成另一个码字时必须改变的最小位数。例如，7 位 ASCII 码增加一位奇偶位成为 8 位的码字，这 128 个 8 位的码字之间的海明距离是 2。所以当其中一位出错便能检测出来。两位出错时就变成另一个码字。如果任意码字之间的海明距离是 d，则所有不大于 d−1 位的错误都可以检查出来，所有少于 d/2 位的错误都可以纠正。对于某种长度的错误串，要纠正它就要用比仅仅检测它多一倍的冗余位。

3. 循环冗余校验码

循环冗余校验码(CRC)是一种循环码，其特征是信息字段和校验字段的长度可以任意选定，在局域网中有广泛应用。

生成 CRC 码的基本原理是：任意一个由二进制位串组成的代码都可以和一个系数仅为 0 和 1 取值的多项式一一对应，如代码 1010111 对应的多项式为 $x^6+x^4+x^2+x+1$。

CRC 码集选择的原则是：若设码字长度为 N 位，信息字段为 K 位，校验字段为 R 位 (N=K+R)，则对于 CRC 码集中的任一码字，存在且仅存在一个 R 次多项式 $g(x)$，使得

$$V(x)=A(x)g(x)=x^R m(x)+r(x)$$

式中，$m(x)$为 K 次信息多项式；$r(x)$为 R−1 次校验多项式。

$$g(x)=g_0+g_1x+g_2x^2+\cdots+g_Rx^R$$

通常将 $g(x)$称为生成多项式，即所有合法的码字都可以由 $g(x)$生成。数据通信的发送方通过指定的 $g(x)$产生 CRC 码字，接收方则通过该 $g(x)$来验证收到的 CRC 码字。根据信息字段和 $g(x)$来生成/验证 CRC 码字的过程可由软件和硬件两种方法实现。

(1) 软件实现的方法借助于多项式除法。

(2) CRC 可以用移位寄存器实现，移位寄存器由 k 位组成，还有几个异或门和一条反馈回路。如图 2-4 所示的移位寄存器可以按 CCITT-CRC 标准生成 16 位的校验和。寄存器被初始化为 0，数据字从右向左逐位输入。当一位从最左边移出寄存器时，就通过反馈回路进入异或门，与后继进来的位以及左移的位进行异或运算。当所有 m 位数据从右边输入完后，再输入 k 个 0(本例中 k=16)。最后，当这一过程结束时，移位寄存器中就形成了校验和。k 位的校验和随在数据位后边发送，接收端可以按同样的过程计算校验和并与接收到的校验和比较，以检测传输中的差错。

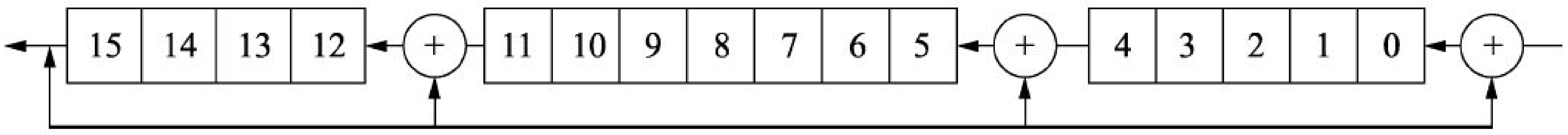


图 2-4 CRC 的实现

推荐的 CRC 生成多项式 $g(x)$为

CRC12=$x^{12}+x^{11}+x^3+x^2+x^1+1$ R=12

$CRC16=x^{16}+x^{15}+x^2+1$　$R=16$　IBM 专用

$CRC16=x^{16}+x^{12}+x^5+1$　$R=16$　CCITT 专用

$CRC32=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$　$R=32$　LAN 中常用

2.9.2　典型例题分析

例 2-18　已知数据信息为 16 位，最少应附加__(3)__位校验位，才能实现海明码纠错。(2017 年上半年真题 3)

A. 3　　B. 4　　C. 5　　D. 6

解析：海明码公式：$2r>k+r+1$，其中 r 为校验位，k 为信息位数，由题意知信息位数为 16，显然 r 至少应为 5。

答案：C

例 2-19　在采用 CRC 校验时，若生成多项式为 $g(x)=x_5+x_2+x+1$，传输数据为 1011110010101 时，生成的帧检验序列是__(28)__。(2016 年下半年真题 28)

A. 10101　　B. 01101　　C. 00000　　D. 11100

解析：CRC 循环冗余校验码利用循环码的误码检测特性进行误码检测，循环码的已编码字可被生成多项式 $g(x)$ 整除，接收端可以利用这一点进行检错，若不能整除，则有错。原始报文为 1011110010101，其生成多项式为：x^5+x^2+x+1，在原始报文后面添加 5 个 0(生成多项式的最高次幂为 5)作为被除数，除以生成多项式所对应的二进制数 100111，模除后得到的余数为校验码 00000。

答案：C

例 2-20　一对有效码字之间的海明距离是__(15)__。如果信息为 10 位，要求纠正 1 位错，按照海明编码规则，最少需要增加的校验位是__(16)__位。(2016 年上半年真题 15、16)

(15) A. 两个码字的比特数之和　　B. 两个码字的比特数之差

　C. 两个码字之间相同的位数　　D. 两个码字之间不同的位数

(16) A. 3　　B. 4　　C. 5　　D. 6

解析：码距就是两个码字 C1 和 C2 之间不同的比特数。如：1100 与 1010 的码距为 2，1111 与 0000 的码距为 4。

校验码个数为 k，2 的 k 次方个校验信息，1 个校验信息用来指出“没有错误”，其余 $2k-1$ 个校验信息指出错误发生在哪一位。但也可能是校验位错误，所以满足 $m+k+1\leqslant 2k$。如果信息位 10 位，要求纠正 1 位错，按照海明编码规则，最少需要增加的校验位是 4 位。

答案：(15) D　(16) B

2.9.3　同步练习

海明码是一种纠错的编码，一对有效码字之间的海明距离是__(1)__。如果信息为 6 位，要求纠正 1 位，按照海明编码规则，需要增加的校验位是__(2)__位。

(1)　A. 两个码字的比特数之和　　B. 两个码字的比特数之差

　C. 两个码字之间相同的比特数　　D. 两个码字之间不同的比特数

(2) A. 3　　B. 4　　C. 5　　D. 6

2.9.4 同步练习参考答案

(1) D　　(2) B

2.10 本 章 小 结

本章知识点在 2014 年的新大纲中改动不大，主要删除了扩频通信知识点，其他只是一些表述方式的调整。

本章主要要求考生掌握数据通信的基础知识，包括信道特性、调制和编码、传输技术、通信方式、同步控制技术、交换技术、多路复用技术、差错控制技术、传输控制技术、传输介质和通信电缆。

本章相关知识点在历次考试中分布相对集中，分值在 4 分左右。本章对数据通信基础知识的学习，关键要建立整体观念，厘清各种数据通信技术的机理和相互间的联系，以常用的典型系统为主线，抓住重点。本章每节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

2.11 达标训练题及参考答案

2.11.1 达标训练题

1. 假设模拟信号的频率范围是 3～9MHz，采样频率必须大于________，才能使得到的样本信号不失真。

A. 6MHz　　B. 12MHz　　C. 18MHz　　D. 20MHz

2. 设信道带宽为 4000Hz，采用 PCM 编码，采样周期为 125μs，每个样本量化为 128 个等级，则信道的数据速率为________。

A. 10kb/s　　B. 16kb/s　　C. 56kb/s　　D. 64kb/s

3. 设信道带宽为 3400Hz，采用 PCM 编码，采样周期为 125μs，每个样本量化为 256 个等级，则信道的数据速率为________。

A. 10kb/s　　B. 16kb/s　　C. 56kb/s　　D. 64kb/s

4. 在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 2 位终止位，每秒钟传送 100 个字符，则有效数据速率为________。

A. 100b/s　　B. 500b/s　　C. 700b/s　　D. 1000 b/s

5. 下列选项中，不采用虚电路通信的网络是________网。

A. X.25　　B. 帧中继　　C. ATM　　D. IP

6. 在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶校验位和 1 位终止位，每秒钟传送 200 个字符，采用 DPSK 调制，则码元速率为__(1)__，有效数据速率为__(2)__。

(1) A. 200 波特　B. 500 波特　C. 1000 波特　D. 2000 波特

(2) A. 200b/s　B. 1000b/s　C. 1400b/s　D. 2000b/s

7. 模拟信号与数字信号的划分是依据________。

A. 幅度上是否离散　B. 时间上是否离散

C. 幅度和时间上是否都离散　D. 幅度或时间上是否离散

8. 语言信号是模拟信号，其标准频谱范围为________。

A. 20～20kHz　B. 300～3400Hz

C. 0～300Hz　D. 109～1010Hz

9. 为了实现长距离传输，模拟传输系统都使用放大器来使信号中的能量得到增加，其噪声分量________。

A. 随之增大　B. 随之减少　C. 保持不变　D. 不一定

10. 若在规定的时间间隔内，最少以高于________的最高有效信号频率的速率对信号 f 进行采样，那么，这些采样值包含了原始信号的全部信息。

A. 1 倍　B. 2 倍　C. 3 倍　D. 4 倍

11. 脉冲代码调制的传输过程是：先将模拟信号采样、量化、编码后变成数字信号，经信道传输到接收端，先由译码器恢复出采样值，再经________滤出模拟基带信号。

A. 低通滤波器　B. 高通滤波器

C. 串并变换器　D. 中继器

12. PCM 对话音的采样速率为 8000 次/秒，这是因为这个速率________。

A. 代表 PCM 技术所能支持的最大速率

B. 确保了唯一性

C. 确保了语言信号能够无失真地重构

D. 通过采样芯片很容易获得

13. ________方式需在两站之间建立一条专用通路。

A. 电路交换　B. 报文交换

C. 虚电路分组交换　D. 数据报分组交换

14. 电路交换最适用的场合为________。

A. 传输信息量较小　B. 实时和交互式通信

C. 传输信息量较大　D. 存储转发方式

15. 电路交换技术中采用时分多路复用进行数据交换，其时隙含________。

A. 53 字节　B. 128 字节　C. 8 比特　D. 8 字节

16. 在数据的分组交换方式中，虚电路技术的主要特点是：在数据传输之前，站与站之间建立________。

A. 专线连接，各节点不需要为每个分组进行路径选择

B. 专线连接，各节点需要为每个分组进行路径选择

C. 逻辑连接，各节点需要为每个分组进行路径选择

D. 逻辑连接，各节点不需要为每个分组进行路径选择

17. 数据报方式中，在保证网络正常通信的情况下，传送到目的站的分组流顺序可能与发送站的发送顺序不同，这是因为_______。

A. 分组流在传送过程中，发生重新排序

B. 各组具有相同目的地址的分组流选择了不同的传输路径

C. 各个分组的传送速率不同

D. 各个分组在传输节点有不同的权限

18. 分组交换与报文交换在形式上的主要区别在于_______。

A. 分组交换的数据单元包括目的地址

B. 分组交换网络限制数据单元的长度

C. 报文交换采用存储转发机制

D. 报文交换可以把一个报文发到多个目的地

19. 在信元交换中，信元的信息域包含的字节数为________。

A. 53　　B. 49　　C. 48　　D. 5

2.11.2 参考答案

1.C	2.C	3.D	4.C
5.D	6.(1) D (2) C	7. C	8. B
9. A	10. B	11. A	12. C
13. A	14. B	15. C	16. D
17. B	18. B	19. C	

第 3 章　广域通信网

大纲要求：

- 公共交换电话网。
- X.25 公共数据网，包括 CCITT X.21 接口、流量控制、HDLC 协议、X.25 PLP 协议。
- 帧中继协议，其中帧中继的格式是重点。
- ISDN 和 ATM，包括 ISDN 的结构、传输模式及 ATM 各层的功能等。

3.1　公共交换电话网

3.1.1　考点辅导

公共交换电话网(Public Switched Telephone Network，PSTN)，从名称上就可以看出这是使用交换技术的网络。事实上，它正是以电路交换技术为基础的，用于传输模拟话音的网络。

1. 电话系统结构

如图 3-1 所示，用户电话通过一对铜线连接到最近的端局。而在应用于数字信号通信时，发送端把数字信号变换为模拟信号，接收端再把模拟信号变换为数字信号。局间干线则传输数字信号。

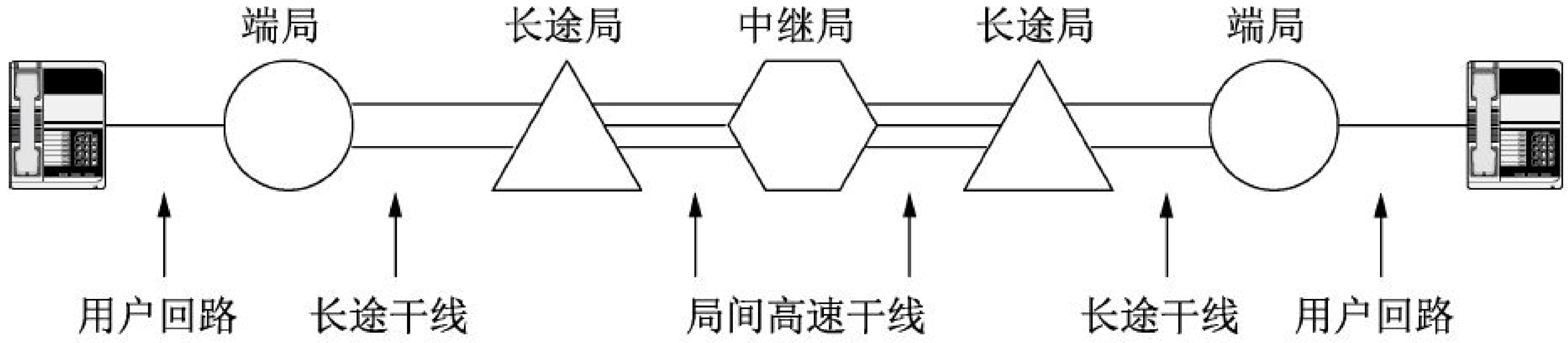


图 3-1　电话系统示意图

2. 本地回路

用户把数据终端或计算机连接到电话网上就可进行通信。按照 CCITT 的术语，用户的数据终端或计算机叫作数据终端设备(DTE)。在通信网络一边，有一个设备管理网络的接口，这个设备称为数据电路设备(DCE)。DCE 通常指调制解调器等，提供建立、维持和拆除电路连接以及波形变换和编码的功能，如图 3-2 所示。

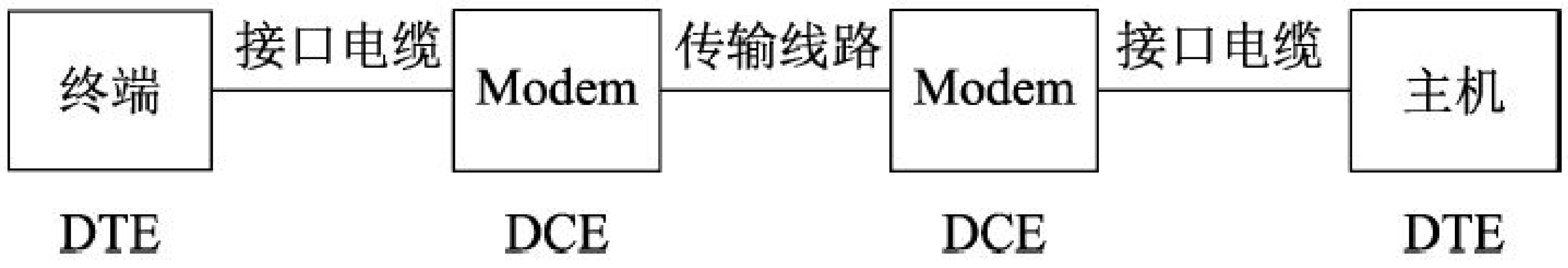


图 3-2　本地回路示意图

3. 调制解调器

调制解调器(Modem)通常由电源、发送电路和接收电路组成。发送电路包括调制器、放大器以及滤波、整形和信号控制电路，它的功能是把计算机产生的数字脉冲转换为已调制的模拟信号；接收电路包括解调器及有关电路，它的作用是把模拟信号变成计算机能接收的数字脉冲。

早期的低速 Modem 采用调频技术。后来的 Modem 采用四进制调相技术，即两比特对应一个相移，也有的 Modem 采用差分相移键控(DPSK)技术。

符合 CCITT V.29 建议的 Modem 以 9600b/s 的速率进行全双工或半双工传输，并且采用正交幅度调制(QAM)技术。QAM 是每个 4 比特组的第一位，用于确定码元的幅度，而其余 3 位用于确定码元的相位。4 种幅度和 8 种相位的结合产生了 16 种不同的码元，因而在 2400 的波特率下可得到 9600b/s 的数据速率。

符合 CCITT V.32 建议的 Modem 使用网格编码调制(TCM)技术。TCM 在 QAM 的基础上，在编码的过程中插入一个冗余比特，这个冗余比特根据卷积码的原理计算。接收端利用冗余比特进行纠错，从而减小误码率。调制器的输入数据流被分成 4 位的比特组，4 位的比特组经过卷积编码产生了第五位——冗余校验位。这种 Modem 可以在公共交换网上实现 9600b/s 的高速传输。

符合 CCITT V.33 建议的 Modem 对 6 比特组进行幅度相位编码，再增加一个冗余位，形成 7 比特网络编码。在 2400 波特率下可达到 14.4kb/s 的数据传输速率。

符合 V.90 建议的 Modem 数据速率可达 56kb/s。这种 Modem 采用非对称的工作方式，从客户端向服务器端发送称为上行信道，数据速率为 28.8kb/s 或 33.6kb/s；从服务器端向客户端发送称为下行信道，数据速率可以达到 56kb/s。

3.1.2　典型例题分析

例 3-1　在 xDSL 技术中，能提供上下行信道非对称传输的技术是__(18)__。(2016 年上半年真题 18)

A. HDSL　　B. ADSL　　C. SDSL　　D. ISDNDSL

解析：数字用户线路(Digital Subscriber Line，DSL)允许用户在传统的电话线上提供高速的数据传输，用户计算机借助于 DSL 调制解调器连接到电话线上，通过 DSL 连接访问因特网络或者企业网络。

DSL 采用尖端的数字调制技术，可以提供比 ISDN 快得多的速率，其实际速率取决于 DSL 的业务类型和很多物理层因素，例如电话线的长度、线径、串扰和噪音等。

DSL 技术存在多种类型，以下是常见的技术类型。

- ADSL：非对称 DSL，上下行流量不对称，一般具有三个信道，分别为 1.544～9Mb/s

的高速下行信道，16～640kb/s 的双工信道，64kb/s 的语音信道。

- SDSL：对称 DSL，用户的上下行流量对称，最高可以达到 1.544Mb/s。
- ISDNDSL：介于 ISDN 和 DSL 之间，可以提供最远距离为 4600～5500m 的 128kb/s 双向对称传输。
- HDSL：高比特率 DSL，是在两个线对上提供 1.544Mb/s 或在三个线对上提供 2.048Mb/s 对称通信的技术，其最大特点是可以运行在低质量线路上，最大距离为 3700～4600m。
- VDSL：甚高比特率 DSL，一种快速非对称 DSL 业务，可以在一对电话线上提供数据和语音业务。

答案： B

例 3-2　ADSL 采用__(18)__技术把 PSTN 线路划分为话音、上行和下行三个独立的信道，同时提供电话和上网服务。采用 ADSL 联网，计算机需要通过__(19)__和分离器连接到电话入户接线盒。(2015 年下半年真题 18、19)

(18) A. 对分复用　　B. 频分复用　　C. 空分复用　　D. 码分多址

(19) A. ADSL 交换机　　B. Cable Modem

C. ADSL Modem　　D. 无线路由器

解析： ADSL 技术采用频分复用技术把普通的电话线分成了电话、上行和下行三个相对独立的信道，从而避免了相互之间的干扰。用户可以边打电话边上网，不用担心上网速率和通话质量下降的情况。理论上，ADSL 可在 5km 的范围内，在一对铜缆双绞线上提供最高 1Mb/s 的上行速率和最高 8Mb/s 的下行速率(也就是我们通常说的带宽)，能同时提供语音和数据业务。

在用户端，用户需要使用一个 ADSL 终端即 ADSL Modem 来连接电话线路。ADSL Modem 的作用是完成数据信号的调制和解调，以便数字信号能在模拟信道上传输。

答案： (18) B　(19) C

3.1.3　同步练习

符合 V.90 建议的 Modem 数据速率可达________。

A. 56kb/s　　B. 50 kb/s　　C. 58 kb/s　　D. 60 kb/s

3.1.4　同步练习参考答案

A

3.2　X.25 公共数据网

3.2.1　考点辅导

X.25 是 20 世纪 70 年代由国际电报电话咨询委员会(CCITT)制定的，其正式名称是“工作在公用数据网上以分组方式工作的数据终端设备(DTE)和数据通信设备(DCE)之间的接口”。

3.2.1.1 CCITT X.21 接口

X.21 建议分为两部分：用于公共数据网同步传输的通用 DTE/DCE 接口和电路交换业务的呼叫控制过程。前者是 X.21 的物理层部分，与建立物理链路有关的操作过程有 4 个特性，即电气特性、机械特性、功能特性和过程特性。

3.2.1.2 流量控制和差错控制

1. 停等协议

工作原理是：发送站发出一帧，然后等待应答信号到达后再发送下一帧；接收站每收到一帧后送回一个应答信号(ACK)，表示愿意接收下一帧，如果接收站不送回应答，则发送站必须等待。

在半双工的点对点链路上，发送一帧的时间为 $T_{FA}=2t_p+t_f$，其中 t_p 为传播延迟，t_f 为发送一帧的时间(称为一帧时)。线路的利用率为

$$E=\frac{t_f}{2t_p+t_f} \tag{3-1}$$

定义 $a=t_p/t_f$，则

$$E=\frac{1}{2a+1} \tag{3-2}$$

线路传播延迟是线路长度 d 和信号传播速率 v 的比值，而一帧时是帧长 L 和数据速率 R 的比，因而有

$$a=\frac{d/v}{L/R}=\frac{Rd/v}{L} \tag{3-3}$$

2. 滑动窗口协议

滑动窗口协议的主要思想是允许连续发送多个帧，而无须等待应答。如果接收端能容纳 W 个帧的缓冲区(即窗口大小为 W)，那么发送端就可以连续发送 W 个帧而不必等待应答信号，但在收到接收端发送的确认信号之前，发送端窗口不会移动。接收端收到一个帧时，就发送一个应答信号，并把窗口滑动到 i～W-i+1 的位置，表明 i 之前的帧已正确接收，期望接收后续的 W 个帧。随着数据传送过程的进展窗口向前滑动，因而取名滑动窗口协议。

滑动窗口协议的效率为

$$E=\frac{Wt_f}{2t_p+t_f}=\frac{W}{2a+1} \tag{3-4}$$

3. 差错控制

利用差错检测技术自动地对丢失帧和错误帧请求重发的技术称为 ARQ(Automatic Repeat reQuest)技术。

1) 停等 ARQ 协议

停等 ARQ 协议是停等流控技术和自动请求重发技术的结合。发送站发送一帧后必须等待应答信号，收到肯定应答信号 ACK 后继续发送下一帧；收到否定应答信号 NAK 后重发该帧；在一定的时间间隔内没有收到应答信号也必须重发。

2) 连续 ARQ 协议

连续 ARQ 协议是滑动窗口技术和自动请求重发技术的结合。由于窗口尺寸开到足够大

时，帧在线路上可以连续地流动，因此又称其为连续 ARQ 协议。根据出错帧和丢失帧处理上的不同，连续 ARQ 协议又分选择重发 ARQ 协议和后退 N 帧 ARQ 协议。

选择重发 ARQ 协议只重发出错的帧，其后面的帧被缓存。采用 ARQ 协议时，窗口的最大值应为帧编号数的一半，即 $W_{发}=W_{收}\leqslant 2k-1$。

后退 N 帧 ARQ 协议是从出错处重发已发过的 N 个帧。窗口的大小限制为 $W\leqslant 2k-1$。

3.2.1.3　HDLC 协议

HDLC(High Level Data Link Control，高级数据链路控制)协议是国际标准化组织根据 IBM 公司的 SDLC 协议扩充开发而成的。它是一种面向位的数据链路控制协议。

HDLC 帧由 6 个字段组成，如图 3-3 所示。

帧标志 F	地址字段 A	控制字段 C	信息字段 INFO	帧校验序列 FCS	帧标志 F
8	8	8	可变长	16或32	8
	可扩展	可扩展			

图 3-3　HDLC 帧结构

(1) HDLC 用一种特殊的位模式 0111110 作为帧的边界标志。

(2) 地址字段用于标识从站的地址，用在点对多点链路中。

(3) HDLC 定义了 3 种帧：信息帧(I 帧)、管理帧(S 帧)和无编号帧(U 帧)，如图 3-4 所示。控制字段第一位或前两位用于区别 3 种不同格式的帧。基本的控制字段是 8 位长。扩展的控制字段为 16 位长。

(4) 信息字段只有 I 帧和某些无编号帧含有的信息字段。

(5) 帧校验序列通常使用 CRC-CCITT 标准产生的 16 位校验序列，有时也使用 CRC-32 产生的 32 位校验序列。

I帧	0	N(S)		P/F	N(R)
S帧	0	1	SS	P/F	N(R)
U帧	1	1	MM	P/F	MMM

图 3-4　HDLC 3 种帧的基本控制信息

3.2.1.4　X.25 PLP 协议

1. 虚电路的建立和释放

X.25 的分组层提供虚电路服务。它支持交换虚电路(Switched Virtual Circuit，SVC)和永久虚电路(Permanent Virtual Circuit，PVC)。

(1) SVC 是在发送方向网络发送请求建立连接报文要求与远程机器通信时建立的。一旦虚电路建立起来，就可以在建立的连接上发送数据，而且可以保证数据正确到达接收方。X.25 同时提供流量控制机制，以防止快速的发送方淹没慢速的接收方。SVC 的特点是灵活，当需要通信时才建立连接。但是，每次建立连接都会耗费时间。

(2) PVC 的用法与 SVC 相同，但它是由用户和长途电信公司经过商议预先建立的，因

而它时刻存在，用户不需要建立链路就可直接使用它。PVC 有点类似于租用的专用线路。PVC 没有 SVC 那样灵活，但是它不需要花费时间建立连接，比较适用于需要及时通信的设备。

图 3-5 示意了 X.25 虚电路建立和释放的过程。

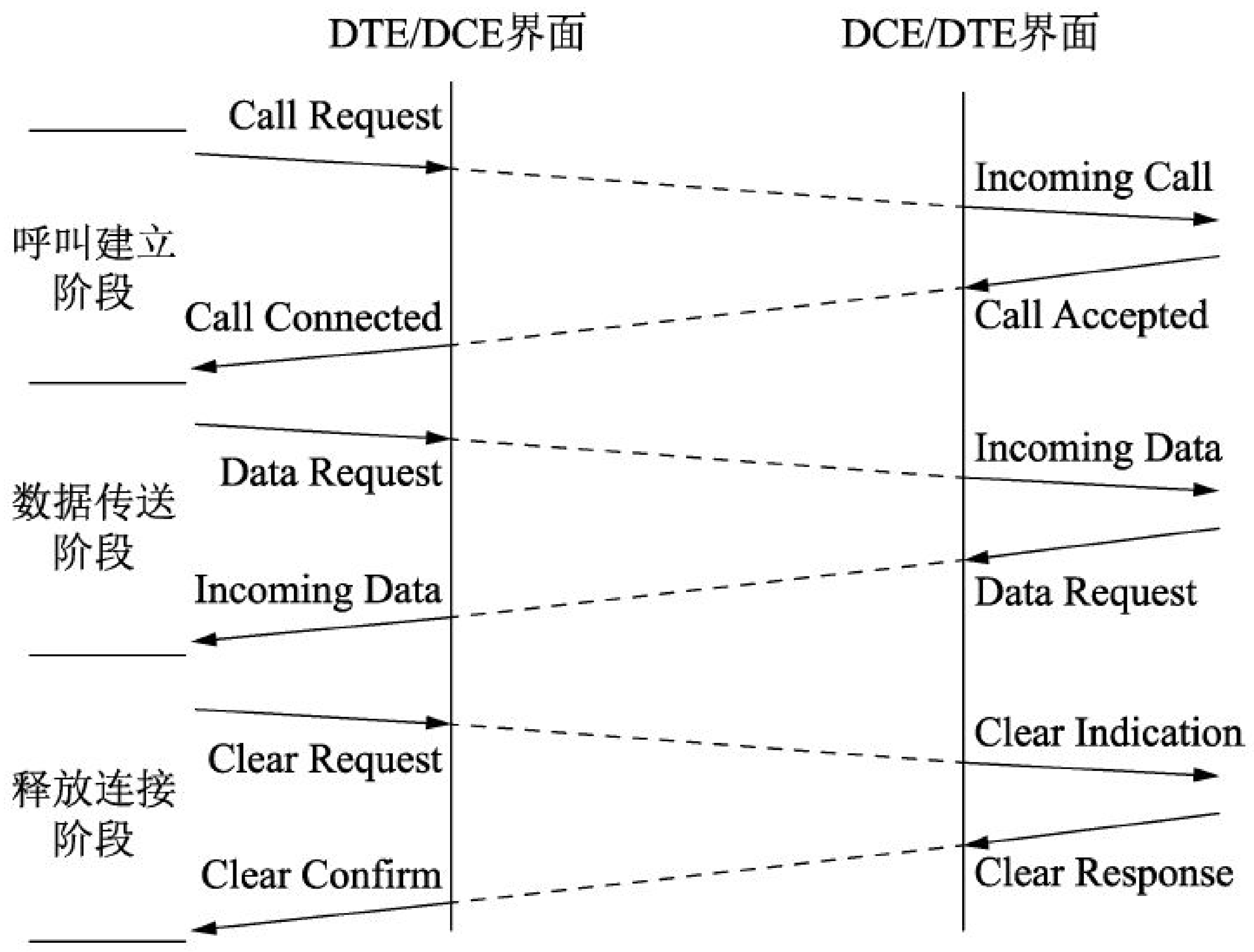


图 3-5　虚电路的建立和释放过程

2. PLP 协议

X.25 网络层采用分组级协议(Packet Level Protocol，PLP)。PLP 协议把用户数据分成一定大小的块(一般为 128 字节)，再加 24 位或 32 位的分组头组成数据分组。分组头中第三个字节的最低位用来区分数据分组(该位为 0)和其他的控制分组(该位为 1)。

X.25 具有分组排序的功能，能识别分组组成的序列。当长的数据块经过一个只允许小分组通过的网络时，要保持数据块的完整性，就需要这一功能。

3. 流量和差错控制

X.25 的流量控制和差错控制机制与 HDLC 类似。X.25 默认的窗口大小是 2，但是对于 3 位顺序号窗口最大可设置为 7，对 7 位的顺序号，窗口最大可设置为 127。这是在建立虚电路时通过协商决定的。X.25 的差错控制采用后退 N 帧 ARQ(自动重发请求)协议。

3.2.2　典型例题分析

例 3-3　Cisco 路由器高速同步串口默认的封装协议是__(12)__。(2015 年上半年真题 12)

A. PPP　　B. LAPB　　C. HDLC　　D. AIM-DXI

解析：在路由器的广域网连接中，应用最多的端口还要算“高速同步串口”(SERIAL)，这种端口主要是用于连接目前应用非常广泛的 DDN、帧中继(Frame Relay)、X.25、PSTN(模拟电话线路)等网络连接模式，SERIAL 端口支持 HDLC、PPP 和 Frame Relay 的广域网封装协议。HDLC 是 CISCO 路由器使用的默认协议，一台新路由器在未指定封装协议时默认使

用 HDLC 封装。

答案：C

3.2.3 同步练习

下面的广域网络中属于电路交换网络的是______。

A. ADSL B. X.25 C. FRN D. ATM

3.2.4 同步练习参考答案

A

3.3 帧 中 继 网

3.3.1 考点辅导

3.3.1.1 帧中继业务

帧中继与 X.25 一样，也支持永久虚电路及交换虚电路。但是相对来说，PVC 使用的比较多一点。用户可以在两个节点之间租用一条永久虚电路并通过该虚电路发送数据帧，其长度可达 1600 字节。用户也可以在多个节点之间通过租用多条永久虚电路进行通信。

在帧中继的虚电路上可以提供不同的服务质量，服务质量参数有以下几个。

- 接入速率(A_R)：指 DTE 可获得的最大数据速率，用户接入网络接口的物理速率。
- 约定突发量(B_c)：指在 T_c 时间间隔内允许用户发送的数据量。
- 超突发量(B_e)：指在 T_c 时间间隔内超过 B_c 部分的数据流量。
- 约定数据速率(C_{IR})：指正常状态下的数据速率，取 T_c 内的平均值。
- 扩展数据速率(E_{IR})：允许用户在 C_{IR} 基础上额外传输的数据速率。
- 约定速率测量时间(T_c)：指测量 B_c 和 B_e 的时间间隔。
- 信息字段最大长度：指每个帧中包含的信息字段的最大字节数，默认为 1600 字节。

这些参数的关系有

$$B_c=T_cC_{IR}$$
$$B_e=T_cE_{IR}$$

3.3.1.2 帧中继协议

帧中继协议称为 LAP-D(D 信道链路接入规程)，它比 LAPB(平衡型链路接入规程)简单，省去了控制字段。帧中继的帧格式如图 3-6 所示。LAP-D 帧头和帧尾都是一个字节的帧标志字段，编码为 01111110，信息字段长度可变，1600 是默认的最大长度。

由于 LAP-D 增加了拥塞控制功能，因此帧格式中 FECN 位、BECN 位及 DE 位就显得比较重要。FECN 位是向前拥塞比特位，该位为 1 表示在传送方向上出现了拥塞，该帧到达

接收方后，接收方可据此调整发送方的数据速率。BECN 位是向后拥塞比特位，该位为 1 表示在与传送相反的方向上出现了拥塞，该帧到达发送端后，发送方可据此调整发送数据速率。DE 位是优先丢弃比特位，在网络发生拥塞时，DE 位为 1 的帧被优先丢弃。

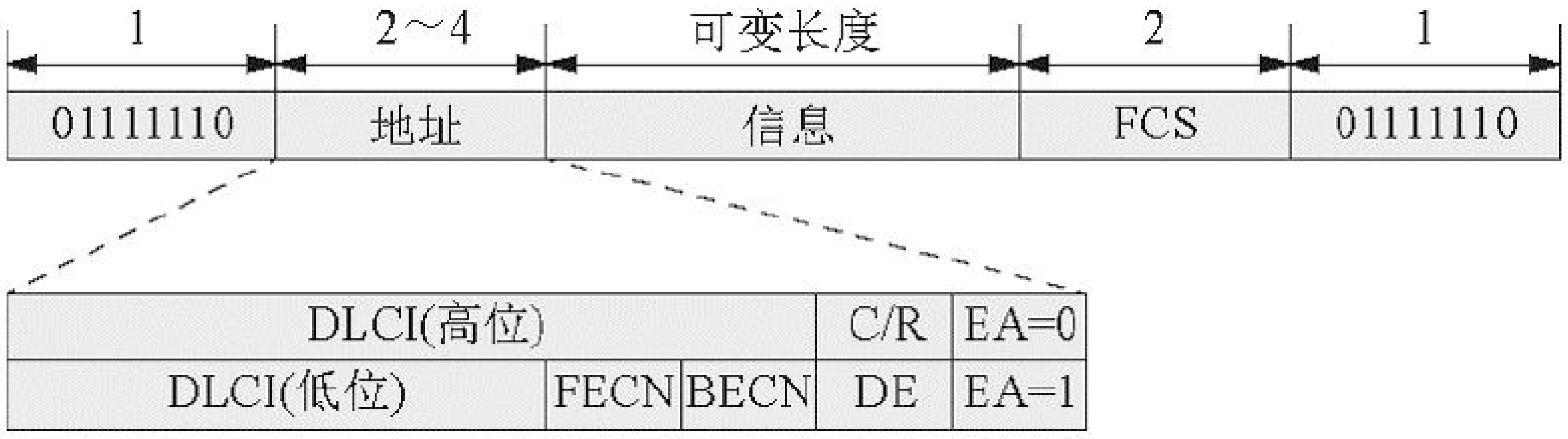


图 3-6　帧中继的帧格式

3.3.1.3　固定虚电路

PVC 管理协议控制端到端的连接，通过属于带外信令的 UI 帧(无编号信息帧)传送，主要有以下 3 项功能。

(1) 周期地检查物理连接的完整性。

(2) 通知给定接口上 PVC 的生成、删除及是否存在。

(3) 通知 PVC 的状态和可利用性。

PVC 管理消息的格式如图 3-7 所示。可以看出，这种帧与 SVC 信令帧的区别是把 I 帧的控制字段换成了 UI 帧的控制字段，其他均相同。用于 PVC 管理的消息类型只有两种，即 STATUS ENQUIRY 和 STATUS，分别用于查询和应答永久虚电路的状态信息。在消息类型后面的信息单元包含 PVC 的详细信息。可以有多个信息单元，每个信息单元对应一条 PVC。

图 3-7　PVC 管理帧格式

PVC 管理协议以轮询方式工作。每隔一段时间进行一次查询和应答，可以使用 3 种应答方式。

(1) 单向信令。这是一种不平衡的信令机制。每隔一段时间(如轮询定时器 T_{391}=10s)，由用户终端向网络发送 STATUS ENQUIRY 查询消息，网络用包含链路完整性的 STATUS 响应。每经过 6 次(即轮询计数器 N_{391}=6)询问，网络将包含所有 PVC 状态的消息送给用户

终端，如图 3-8 所示。

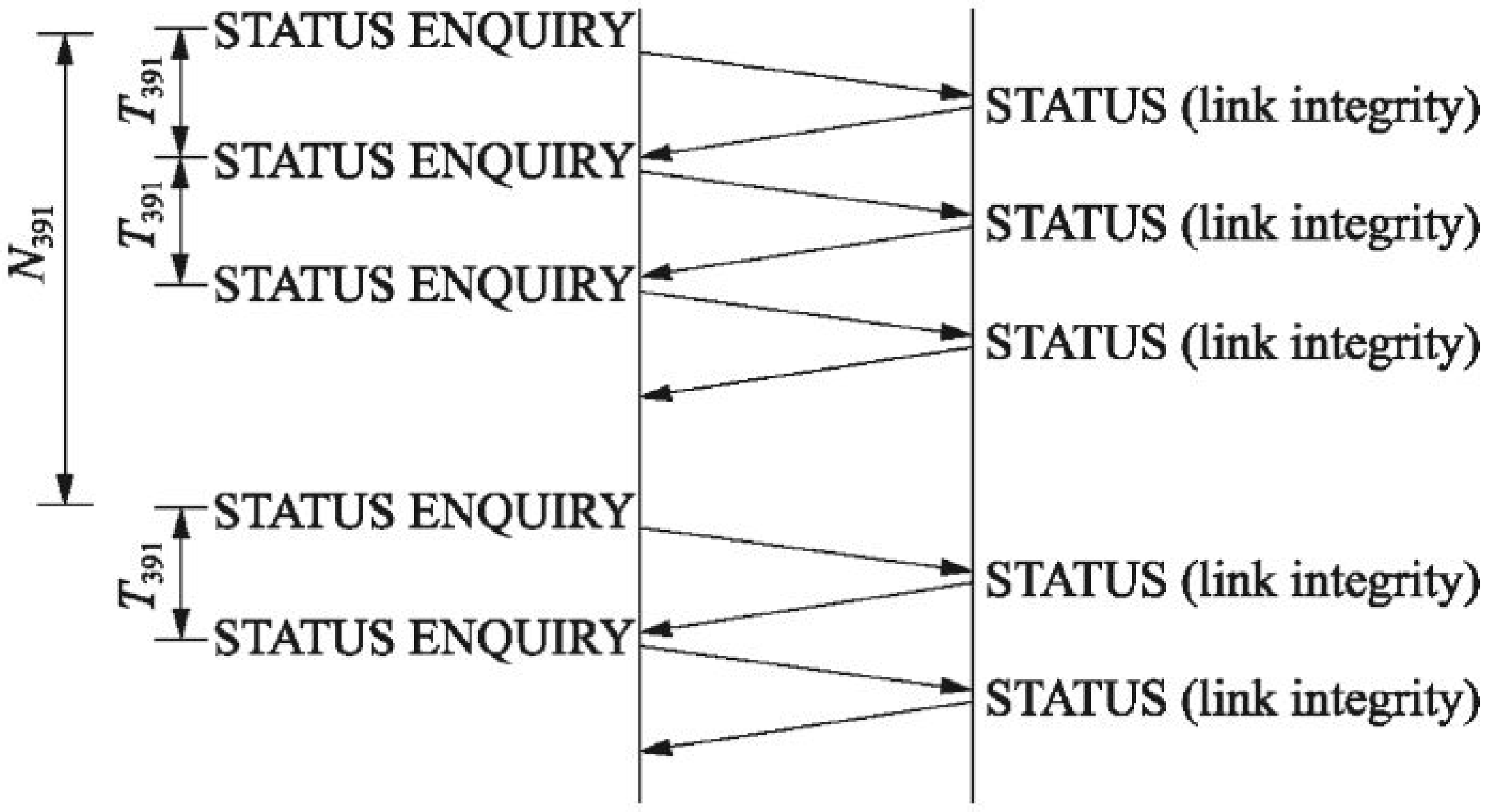


图 3-8　周期轮询

(2) 双向信令。这是一种平衡信令机制，用在网络与网络之间互相询问和应答，如图 3-9 所示。询问周期仍然是 T_{391}s，同时任一方每隔 N_{391} 个周期后都可以请求一个全状态报告。

由于双方独立地询问，因此可以各自使用不同的 T_{391} 和 N_{391} 参数。

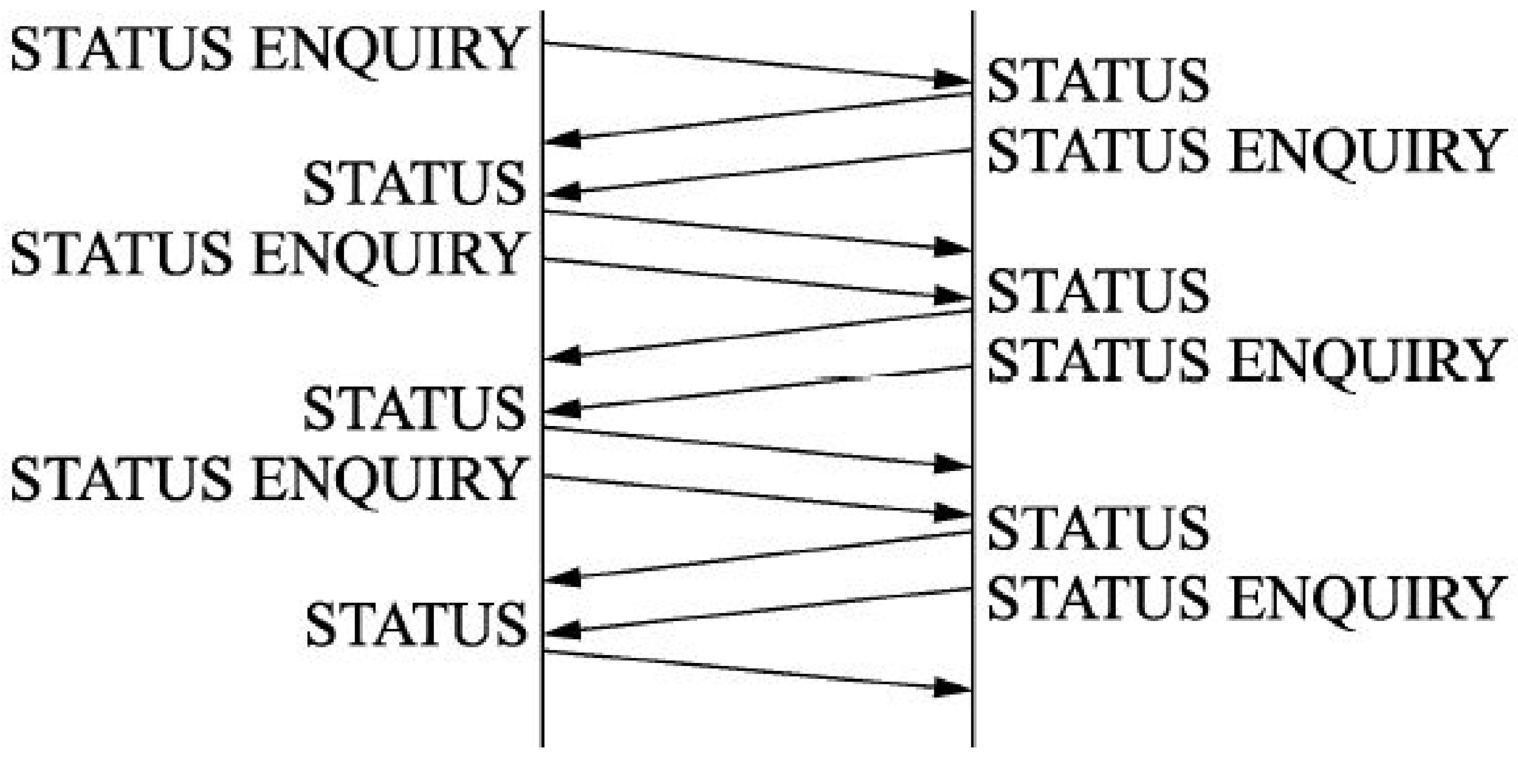


图 3-9　双向轮询

(3) 异步更新信令。即异步发送 PVC STATUS 消息，其中只包含一条 PVC 的状态信息单元。由于这种消息不需要询问，因此不受询问周期的限制，可以及时报告 PVC 的状态。

3.3.1.4　帧中继的应用

帧中继标准已渐成熟，业务需求不断增加，目前已进入高速发展时期。帧中继可通过 X.25 更新软件实现，可在 DDN 上配置端口实现。在以 ATM 为主干的网络中，帧中继仍然可以作为良好的用户接入方式。

目前的路由器都支持帧中继协议，帧中继上可承载流行的 IP 业务，IP 加帧中继已经成了广域网应用的绝佳选择。近年来，帧中继上的话音传输技术(VOFR)也不断发展。

帧中继远程联网的主要优点如下。

- 基于分组(帧)交换的透明传输，可提供面向连接的服务。
- 帧长可变，长度可达 1600～4096 B，可以承载各种局域网的数据帧。
- 数据速率可达 2～45Mb/s。
- 既可以按需要提供带宽，也可以应付突发的数据传输。

- 没有流控和重传机制，开销很少，传输效率高。

帧中继可以有效地处理突发性数据，当数据业务量为突发性时，由于帧中继具有动态分配带宽的功能，因此允许用户的数据速率在一定范围内变化。但它不适于对延迟较敏感的应用(如音频、视频)，因为无法保证可靠提交。

3.3.2 典型例题分析

例 3-4 下面关于帧中继的描述错误的是__(20)__，思科路由器支持的帧中继本地管理接口类型(Lmi-type)不包括__(21)__。(2014 年下半年真题 20、21)

(20) A. 在第三层建立虚电路

B. 提供面向连接的服务

C. 是一种高效率的数据链路技术

D. 充分利用了光纤通信和数字网络技术的优势

(21) A. Cisco　　B. OCE　　C. ANSI　　D. Q933A

解析：帧中继（Frame Relay, FR)网络运行在 OSI 参考模型的物理层和数据链路层。FR 用第二层的帧承载数据业务，因而第三层被省掉了。帧中继提供面向连接的服务，在互相通信的每对设备之间都存在一条定义好的虚电路，并且指定了一个链路识别码 DLCI。帧中继利用了光纤通信和数字网络技术的优势，FR 帧层操作比 HDLC 简单，只检查错误，不再重传，没有滑动窗口式的流量控制机制，只有拥塞控制。所以，帧中继比 X.25 具有更高的传输效率。

普通路由器就可以配置成帧中继交换机。在路由器串行接口配置 FR 封装的命令如下表所示，可设置的本地管理接口类型有 3 种{ANSI|Cisco|Q933A}

命　令	功　能
encapsulation frame-relay[ietf]	设置 Frame Relay 封装
Frame-relay 1mi-type{ansi | cisco | q933a}	设置 Frame Relay LMI 类型
interface interface-type interface-number subinterface-number [multipoint | point-to-point]	设置子接口
frame-relay map protocol protocol-address dlci [broadcast]	映射协议地址与 DLCI
frame-relay interface-dlci dlci[broadcast]	设置 FRDLCI 编号

答案：(20) A　　(21) B

3.3.3 同步练习

1. 以下关于帧中继网络的叙述中，错误的是______。

A. 帧中继提供面向连接的网络服务

B. 帧在传输过程中要进行流量控制

C. 既可以按需提供带宽，也可以适应突发式业务

D. 帧长可变，可以承载各种局域网的数据帧

2. 下面关于帧中继网络的描述中，错误的是______。

A. 用户的数据速率可以在一定的范围内变化
B. 既可以适应流式业务，又可以适应突发式业务
C. 帧中继网可以提供永久虚电路和交换虚电路
D. 帧中继虚电路建立在 HDLC 协议之上

3.3.4 同步练习参考答案

1. B　　2. D

3.4 ISDN 和 ATM

3.4.1 考点辅导

3.4.1.1 综合业务数字网

综合业务数字网(ISDN)是一种数字交换电话系统，它不仅支持电话网上的所有业务，还能够提供数据透明传送业务和分组传送业务。

ISDN 的中心思想是数字比特管道，它是客户和电信公司之间概念上的管道，比特流就从这里流过。在交换技术上，这种网络既支持线路交换，也支持分组交换。

ISDN 的系统结构由 3 部分组成，分别是设备终端、网络终端和适配器。

设备终端(TE)有两种类型：TE1 和 TE2。前者可以和网络终端设备(NT)连接；后者被称为非 ISDN 设备，必须通过终端适配器(TA)才能把 TE2 连接到 NT 上面。

网络终端(NT)配置在用户端，通过用户端与网络端的交换设备相连接。为了满足不同的配置要求，NT 可以分为两种类型：NT1 和 NT2。

- NT1 是第一网络终端，被放置在用户设备和 ISDN 交换系统之间，不仅起到插板作用，还可以进行网络管理和维护等工作。
- NT2 具有交换和集线功能。

ISDN 包括两种，即窄带 ISDN(N-ISDN)和宽带 ISDN(B-ISDN)。平常所说的 ISDN 就是 N-ISDN，它是基于异步传输方式的技术。和 N-ISDN 一样，B-ISDN 包括 N-ISDN 的所有业务功能，它的主要任务就是要以全新的交换体制来支持所有可能的电信业务。

ISDN 定义了一些标准化的通路，定义的标准如下。

- A 通路：4kHz 带宽的标准模拟通路。
- B 通路：64kb/s 的数字 PCM(脉码调制)话音或者数据通路。
- C 通路：8kb/s 或 16kb/s 的数字通路。
- D 通路：16kb/s 或 64kb/s 用作带外信令的数字通路。
- E 通路：64kb/s 为内部 ISDN 信令使用的数字通路。
- H 通路：384kb/s、1358kb/s 或 1290kb/s 的数字通路。

另外，它还提供了两种标准的用户—网络接口，分别是基本速率接口和机群速率接口。基本速率接口允许用户使用模拟电话并且进行数据的纯数字通信，由两条 64kb/s 的 B 信道

和一条 16kb/s 的 D 信道组成，合计的速率是 144kb/s。

1. 窄带 ISDN

窄带 ISDN (N-ISDN)是一种基于电路交换网的技术，目的是以数字系统代替模拟电话系统，把音频、视频和数据业务在一个网络上一同传输。N-ISDN 以固定的比特速率向用户提供电路交换服务、分组服务和其他服务。

N-ISDN 系统提供两种用户接口，即基本速率(2B+D)和一次群速率(30B+D)。其中，B 信道是 64kb/s 的话音或数据信道，D 信道是 16kb/s 的信令信道。用户最多在 NT1 总线上挂接 8 台设备，共享 2B+D 的 144kb/s 信道。大型用户通过 NT2 接入 N-ISDN，享有 30B+D 达到 2.048Mb/s 的速率。N-ISDN 采用的是时分多路复用技术。

N-ISDN 具有类似于 OSI 的 3 层结构。多路复用属于物理层的功能；ISDN 的数据链路层采用 LAPD 协议；网络层主要支持电路交换和分组交换功能，与 X.25 的分组层协议极为相似。

N-ISDN 的缺点是数据传输速率太低，不适合传输视频信息等需要高带宽的应用。

2. 宽带 ISDN

宽带 ISDN(B-ISDN)模型采用了与 OSI 同样的分层概念，同时还以不同的平面来区分用户信息、控制信息和管理信息。用户平面提供与用户数据传送有关的流量控制和差错检测功能；控制平面主要用于连接和信令信息的管理；管理平面支持网络管理和维护功能。

B-ISDN 的关键技术是异步传输模式(ATM)，采用五类双绞线或光纤传输，数据速率可达 155Mb/s。

3.4.1.2 ATM

ATM 即异步传输模式。

1. 同步传输模式与异步传输模式

1) 同步传输模式(STM)

在同步时分多路复用中，不同的子信道通过帧内时间片位置予以区分，基于子信道的信息传输周期性地占用帧中的固定时间片，只要收、发双方在时间上严格保持同步，双方就可以从复用的信道中分解出所需的信息。同步传输模式最大的特点是时间片的静态分配，而空闲时间片浪费了信道的带宽。

当同步传输模式技术引入交换机时，出现了同步时分交换技术，将输入端口的某个时间片的内容“交换”到输出端对应的时间片中。

2) 异步传输模式(ATM)

以异步时分复用概念为基础，每个时间片没有固定的占有者，各子信道的信息按照优先级和排队规则按需分配时间片。为了使得接收方可以区分使用时间片的信息所属，信息的前部增加了报头。报头和信息构成了信道上传输的分组。异步传输模式中的分组定义为 53 字节，也称为信元。ATM 是以信元为传输单位的统计复用技术。

当异步传输模式技术引入交换机时，出现了 ATM 交换技术，根据输入端口的各个信元的信元头中的信息将信元“交换”到指定的输出端口。

采用 ATM 交换技术构造的网络称为 ATM 网络。

2. ATM 体系结构

ATM 网络主要含物理层和数据链路层。其中，数据链路层又被划分为两个子层：ATM 适配子层(AAL)和 ATM 子层。AAL 子层主要定义高层 PDU 和信元中数据域(48 字节)的装拆方法。ATM 子层主要定义信元头的结构以及 ATM 信元的组织结构等。ATM 物理层主要定义物理设备和物理媒体的接口以及信元的传输编码等。

1)　ATM 物理层

ATM 物理层又分为两个子层：物理介质相关子层(PMD)和传输汇聚子层(TC)。PMD 子层负责在物理媒体上正确传输和接收比特流。TC 子层实现信元流和比特流的转换。

2)　ATM 层

ATM 层是 ATM 数据链路层的下子层，主要定义信元头的结构以及使用物理链路的方法。

(1)　信元头结构。

ATM 层定义了两种信元头结构：网络用户端接口(UNI)定义了 ATM 交换机面向用户的信元头格式；网络/网络端接口(NNI)定义了 ATM 交换机之间的接口信元头格式。在两种信元头格式中，VPI 用来标识不同的虚拟路径，VCI 用来标识虚拟路径中的虚拟通道。VPI/VCI 在用户建立连接时分配，并在信息传输途径的 ATM 交换节点上建立输入/输出映射表。传输信元时，交换机根据信元头的 VPI/VCI 查映射表，形成新的 VPI/VCI，填入信元头，物理层的 TC 子层形成新的循环冗余校验码，并通过媒体进行传输。

(2)　ATM 层的功能。

ATM 层提供下列功能：信元的汇集和分拣；VPI/VCI 的管理；信元头的增删；信元速率调整。

3)　ATM 适配层(AAL)

AAL 的主要目的是将高层的信息转换成适合 ATM 网络传输要求的格式。

(1)　CCITT 通信业务分类。

①　CLASS A。支持源/宿之间具有实时性要求的恒定位速率(CBR)业务。CBR 业务采用面向连接的工作方式。

②　CLASS B。支持源/宿之间具有实时性要求的可变位速率(VBR)业务。VBR 业务采用面向连接的工作方式。

③　CLASS C。支持源/宿之间无实时性要求的可变位速率(VBR)业务。

④　CLASS D。支持面向无连接的数据传输服务。

其中，CLASS A/B 支持实时信息的传输(如视频和语音传输)，CLASS C/D 支持非实时要求的信息传输(如高速数据传输)。

(2)　AAL 协议类型。

为了支持上述 4 种类别的业务，CCITT 定义了 4 种类型的 AAL 协议，如表 3-1 所示。

表 3-1　AAL 的分类

项　目	AAL1	AAL2	AAL3/4	AAL5
连接模式	面向连接	面向连接	面向无连接	面向连接
端到端定时	要求	要求	不要求	不要求

续表

位速率	恒定	可变	可变	可变
业务类型	CLASS A	CLASS B	CLASS C/D	CLASS C/D

3.4.2 典型例题分析

例 3-5 下列分组交换网络中，采用的交换技术与其他 3 个不同的是__(18)__网。(2017年下半年真题 18)

A. IP　　B. X. 25　　C. 帧中继　　D. ATM

解析： X.25、帧中继、ATM 均是面向连接的方式。

答案： D

3.4.3 同步练习

1. ATM 高层定义了 4 类业务，压缩视频信号的传送属于______。

A. CBR　　B. VBR　　C. UBR　　D. ABR

2. 下列语句中准确地描述了 ISDN 接口类型的是______。

A. 基群速率接口(30B+D)中的 D 信道用于传输用户数据和信令，速率为 16kb/s
B. 基群速率接口(30B+D)中的 B 信道用于传输用户数据，速率为 64kb/s
C. 基本速率接口(2B+D)中的 D 信道用于传输信令，速率为 64kb/s
D. 基本速率接口(2B+D)中的 D 信道用于传输用户数据，速率为 16kb/s

3. N-ISDN 有两种接口：基本速率接口(2B+D)和基群速率接口(30B+D)，有关这两种接口的描述中，正确的是______。

A. 基群速率接口中，B 信道的带宽为 16kb/s，用于发送用户信息
B. 基群速率接口中，D 信道的带宽为 16kb/s，用于发送信令信息
C. 基本速率接口中，B 信道的带宽为 64kb/s，用于发送用户信息
D. 基本速率接口中，D 信道的带宽为 64kb/s，用于发送信令信息

3.4.4 同步练习参考答案

1. B　2. D　3. C

3.5 本 章 小 结

本章知识点在 2009 年的新大纲中改动不大，主要是一些表述方式的调整。

本章主要要求考生掌握几种典型的广域通信网络及广域通信网络的相关基本概念，主要有公共交换电话网、X.25 公共数据网、CCITT X.21 接口、流量控制、HDLC 协议、X.25

PLP 协议、帧中继协议，ISDN 和 ATM，ISDN 的结构、传输模式以及 ATM 各层的功能等知识。

本章相关知识点在历次考试中都会涉及，分值在 4 分左右。对于本章的学习，考生要牢牢把握大纲中的知识点，仔细分析典型例题及其分析过程。本章前几节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

3.6　达标训练题及参考答案

3.6.1　达标训练题

1. 路由器与计算机串行接口连接，利用虚拟终端对路由器进行本地配置的接口是 __(1)__，路由器通过光纤连接广域网的接口是 __(2)__。

(1)、(2)　A. Console 口　　B. 同步串行口
　　　　C. SFP 端口　　D. AUX 端口

2. 由于内网 P2P、视频流媒体、网络游戏等占用流量过大，影响网络性能，可以采用______来保障正常的 Web 及邮件流量需求。

A. 网闸　　B. 升级核心交换机
C. 部署流量控制设备　　D. 部署网络安全审计设备

3. 以下叙述中，不属于无源光网络优势的是______。

A. 设备简单，安装维护费用低，投资相对较小
B. 组网灵活，支持多种拓扑结构
C. 安装方便，不需要另外租用或建造机房
D. 无源光网络适用于点对点通信

4. 通过电话网传输数据的主要问题是______。

A. 可靠性　　B. 灵活性　　C. 经济性　　D. 话路质量

5. 从 OSI 参考模式来看，ISDN 系统中的 NT1 是一个______。

A. 物理层设备　　B. 数据链路层设备
C. 网络层设备　　D. 传输层设备

6. 在 ISDN 系统结构中，用于家庭的配置，在符合 ISDN 标准的用户设备和 ISDN 交换系统之间应______。

A. 放置 NT2　　B. 放置 NT1
C. 放置 CBX　　D. 放置 NT1 和 NT2

7. ISDN 的标准定义是：由______发展起来的一个网络，提供端到端的______，以支持广泛的服务，包括声音和非声音的，用户的访问是通过______实现的。

A. 综合数字电话网　模拟连接　标准接口
B. STN　模拟连接　标准接口
C. 综合数字电话网　数字连接　标准接口
D. PSTN　数字连接　标准接口

8. CCITT 对 ISDN 定义了两种标准接口：BRI 和 PRI。下面的表述正确的是_______。
   A. ISDN 的 BRI 服务提供了两个 B 信道和一个 D 信道(2B+D)。B 信道的速率为 64kb/s，用于传输用户数据；D 信道的速率为 16kb/s，仅用于传输控制信息和信号信息
   B. D 信道的信号协议对应 OSI 参考模型的第一层到第二层
   C. 在欧洲，ISDN 的 PRI 服务提供 30 个 B 信道和 1 个 D 信道，总的接口速率为 2.048Mb/s
   D. 在北美和日本，ISDN 的 PRI 服务提供 23 个 B 信道和 1 个 D 信道，总的接口速率为 1.544Mb/s，其中 D 信道的速率为 16kb/s
9. ATM 网是一种高速网技术，其核心技术主要取决于_______技术。
   A. 光纤通信　　B. 同步时分多路复用
   C. 异步时分多路复用　　D. 差错控制
10. 帧中继最多可传送_______字节的数据帧。
   A. 1600　　B. 53　　C. 9188　　D. 1500
11. 下面的说法中，_______是错误的。
   A. 帧中继虚电路实现帧中继数据包交换网络中 DTE 间的逻辑连接
   B. SVC 是一种临时连接，在帧中继网络中传输突发性数据
   C. 帧中继的数据链路连接标识符(DLCI)是端到端的
   D. 帧中继的流控由高层协议完成
12. 分组交换结合了_______和_______的优点，将信息分成较小的分组进行_______，动态分配线路的带宽。
   A. 线路交换　报文交换　存储转发
   B. 快速分组交换　报文交换　实时转发
   C. 帧交换　线路交换　存储转发
   D. 线路交换　帧交换　实时转发
13. 下面关于分组交换的叙述，_______是错误的。
   A. 数据报方式灵活、快速
   B. 有数据报和虚电路两种方式
   C. 传输数据的出错率较高，线路利用率低
   D. 虚电路方式能在一条物理链路上建立若干条逻辑上的虚电路，使用户感觉到仿佛有若干条物理链路一样
14. 下面关于 X 系列建议的说法，_______是错误的。
   A. X.21 接口定义了数据终端设备 DTE 到 DCE 的物理和电气接口
   B. X.25 提供点对点的数据发送，而不是一点对多点的发送
   C. X.25 的分组要包含源地址和目的地址的信道鉴别
   D. X.25 网开销较大，在一个分组的传输路径上的每个节点都必须完整地接收一个分组，并且在发送之前完成差错检查
15. 下面关于 ATM 网基本原理的说法，_______是错误的。
   A. ATM 采用虚拟通道模式，通信通道用一个逻辑号标识

B. 通道的标识基于两种标识符，即 VPI 和 VCI

C. 每个 VP 可以用复用方式容纳多达 65 535 个 VC

D. ATM 对信元在网络中传送期间出现的一切问题要进行相关处理

16. ATM 连接管理控制的目的是解决 VC、VP 连接是被接收还是被拒绝的问题。下列______不是有关连接被接收的条件。

A. 有足够的网络资源可以用来建立端到端的连接

B. 能够保证要求的服务质量

C. 可能会影响其他已存在的连接的服务质量，但不严重

D. 不能影响其他已存在的连接的服务质量

3.6.2 参考答案

1. (1) A　(2) C	2. C	3. D	4. D	5. A	
6. B	7. C	8. C	9. C	10. A	
11. C	12. A	13. C	14. C	15. D	16. C

第 4 章　局域网与城域网

大纲要求：

- IEEE 体系结构。
- 以太网。
- 网络连接设备。
- 高速 LAN 技术。
- VLAN。
- CSMA/CA。

4.1　局域网技术概论

4.1.1　考点辅导

4.1.1.1　拓扑结构和传输介质

1. 总线拓扑

总线是一种多点介质，所有的站点都通过接口硬件连接到总线上。工作站发出的数据组成帧，数据帧沿着总线向两端传播，到达末端的信号被终端匹配器吸收。数据帧中含有源地址和目标地址，每个工作站都监视总线上的信号，并复制发给自己的数据。由于总线是共享介质，多个站同时发送数据时会产生冲突，因此需要一种解决冲突的介质访问协议。传统的轮询方式不适合分布式控制，通常采用分布式竞争发送的访问控制方式。

适用于总线拓扑的传输介质有双绞线、同轴电缆和光纤。双绞线价格便宜，便于安装，同轴电缆和光纤则能提供更高的数据速率，连接更多的设备，传输的距离也更远。

同轴电缆分为传播数字信号的基带同轴电缆和传播模拟信号的宽带同轴电缆。宽带电缆比基带电缆传输的距离更远，还可以使用频分多路技术提供多个信道和多种数据传输业务，主要用在城域网中；基带系统主要用于室内或建筑物内部联网。

1)　基带系统

保持数据的原样进行传输称为基带传输或基带数字信号传输。此时的数字信号为电脉冲或者光脉冲。由于数据的波谱具有直流至高频的频谱特性，数字信号传输将占用整个信道的带宽。

通常数据信号的传输会随着距离的增加而衰减，随着频率的增加容易发生畸变，因此，基带传输不适合高速和远距离的传输，除非传输介质的性能很好。

2)　宽带系统

宽带在数据通信领域通常指数据传输速率超过 1Mb/s 的传输系统。宽带传输的特征是

模拟信号传输，因此，宽带传输系统也指宽带模拟信号传输系统。显然，当采用宽带传输技术时，应当采用适当的调制解调技术。

在局域网环境中，宽带传输常采用频分多路复用的技术，支持多路信号的传输。与基带传输相比较，宽带传输可以提供较高的传输速率和抗干扰的能力。

3)　载波带

载波带或单信道宽带是宽带系统的一种简化形式。载波带的整个带宽都贡献给单独的传输信道。一般来说，单信道宽带系统具有下列特点：总线拓扑结构和双向传输。因而传输系统中不能用放大器，也不需要端头，使用载波频率较低的 FSK 调制，因为低频的信号畸变较小。

2. 环型拓扑

环型拓扑由一系列首尾相接的中继器组成，每个中继器连接一个工作站。中继器是一种简单的设备，它能从一端接收数据，然后从另一端发出数据。整个环路是单向传输的。

工作站发出的数据组成数据帧。在数据帧的帧头部分含有源地址和目的地址字段以及其他控制信息。数据帧在环上循环时被目标站复制，返回发送站后被回收。由于多个站共享环上的传输介质，因此需要某种访问逻辑来控制各个站的发送顺序。

由于环网是一系列点对点链路串接起来的，因此可使用任何传输介质。最常用的介质是双绞线，因为它的价格较低；使用同轴电缆可得到较高的带宽，而光纤则能提供更高的数据速率。

3. 星型拓扑

星型拓扑中有一个中心节点，所有的站都连接到中心节点上。电话系统就采用了这种拓扑结构，多终端联机通信系统也是星型结构的例子。中心节点在星型网络中起到控制和交换的作用，是网络中的关键设备。

用星型拓扑结构也可以构成分组广播式的局域网。在这种网络中，每个站都用两对专线连接到中心节点上，一对用于发送，一对用于接收。中心节点叫作集线器，简称 Hub。Hub 接收工作站发来的数据帧，然后向所有的输出链路广播出去。当有多个站同时向 Hub 发送数据时就会产生冲突，这种情况和总线拓扑中的竞争发送一样，因而总线网的介质访问控制方法也适用于星型网。

4.1.1.2　LAN/MAN 的 IEEE 802 标准

IEEE 802 委员会的任务是制定局域网和城域网标准，目前有 20 多个分委员会，它们研究的内容如下。

(1)　802.1：研究局域网体系结构、寻址、网络互联和网络管理。

(2)　802.2：研究逻辑链路控制子层(LLC)的定义。

(3)　802.3：研究以太网介质访问控制协议 CSMA/CD 及物理层技术规范。

(4)　802.4：研究令牌总线网(Token-Bus)的介质访问控制协议及物理层技术规范。

(5)　802.5：研究令牌环网(Token-Ring)的介质访问控制协议及物理层技术规范。

(6)　802.6：研究城域网介质访问控制协议 DQDB 及物理层技术规范。

(7)　802.7：宽带技术咨询组，提供有关宽带联网的技术咨询。

(8) 802.8：光纤技术咨询组，提供有关光纤联网的技术咨询。

(9) 802.9：研究综合声音数据的局域网(IVD LAN)介质访问控制协议及物理层技术规范。

(10) 802.10：网络安全技术咨询组，定义了网络互操作的认证和加密方法。

(11) 802.11：研究无线局域网(WLAN)的介质访问控制协议及物理层技术规范。

(12) 802.12：研究需求优先的介质访问控制协议(100VG-AnyLAN)。

(13) 802.14：研究采用线缆调制解调器(Cable Modem)的交互式电视介质访问控制协议及物理层技术规范。

(14) 802.15：研究采用蓝牙技术的无线个人网(Wireless Personal Area Network，WPAN)技术规范。

(15) 802.16：宽带无线接入工作组，开发 2～66GHz 的无线接入系统空中接口。

(16) 802.17：弹性分组环(Resilient Packet Ring，RPR)工作组，制定了弹性分组环网访问控制协议及有关标准。

(17) 802.18：宽带无线局域网(Radio Regulatory)技术咨询组。

(18) 802.19：多重虚拟局域网共存(Coexistence)技术咨询组。

(19) 802.20：移动宽带无线接入(Mobile Broadband Wireless Access，MBWA)工作组，正在制定宽带无线接入网的解决方案。

(20) 802.21：研究各种无线网络之间的切换问题，正在制定与介质无关的切换业务(Media Independent Handover，MIH)标准。

(21) 802.22：无线区域网(Wireless Regional Area Network，WRAN)工作组，正在制定利用感知无线电技术，在广播电视频段的空白频道进行无干扰无线广播的技术标准。

由于局域网是分组广播式网络，网络层的路由功能是不需要的，因此在 IEEE 802 标准中，网络层简化为上层协议的服务访问点(SAP)。又由于局域网使用多种传输介质，而介质访问协议又与具体的传输介质和拓扑结构有关，因此 IEEE 802 标准把数据链路层划分成两个子层。与物理介质相关的部分称为介质访问控制(Media Access Control，MAC)子层，这个子层提供标准的 OSI 数据链路层服务。局域网的物理层规定了传输介质及其接口的电气特性、机械特性、接口电路的功能以及信令方式和信号速率等。整个局域网的标准以及与 OSI 参考模型的对应关系如图 4-1 所示。

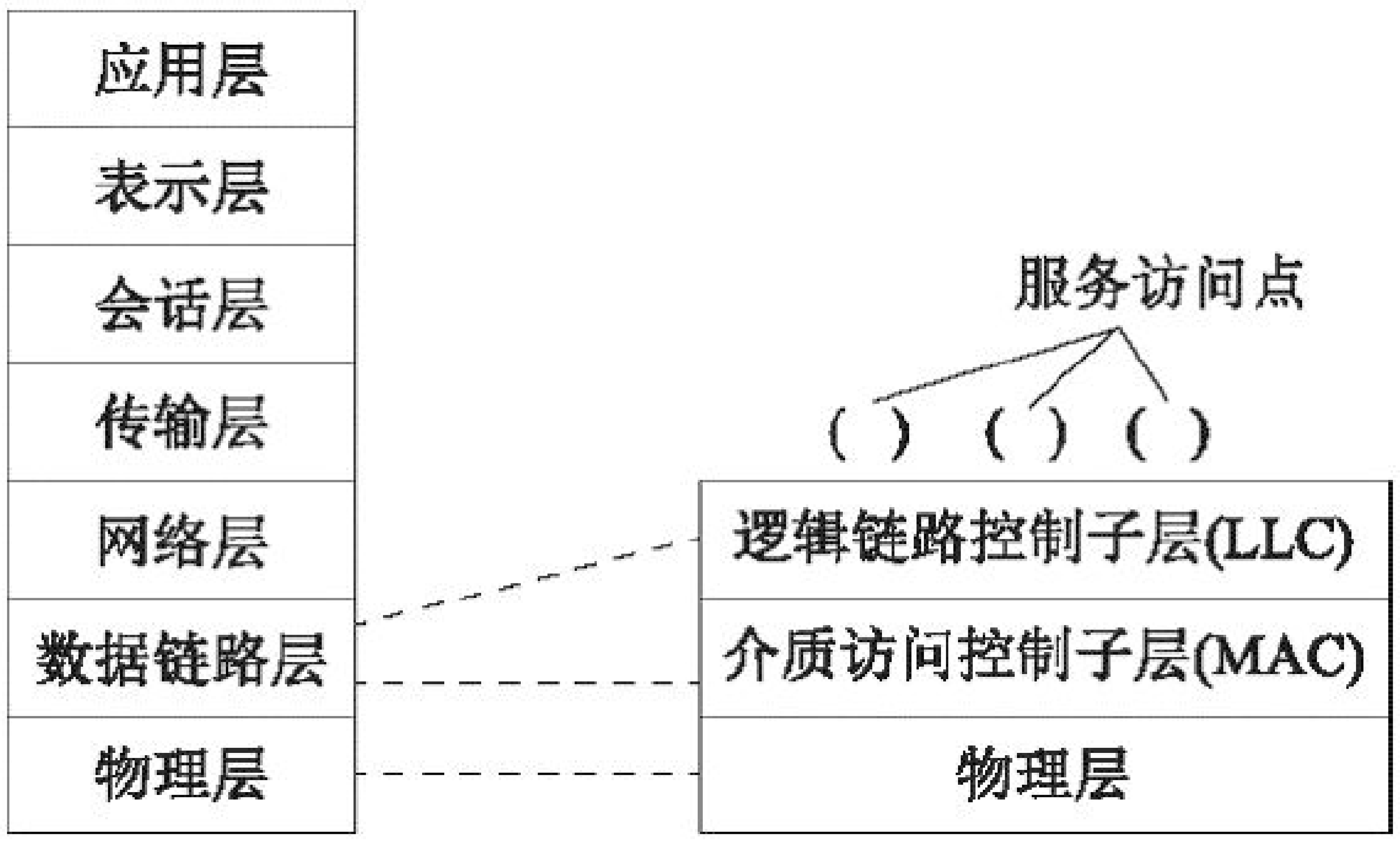


图 4-1　局域网体系结构与 OSI/RM 的对应关系

局域网的体系结构也说明在数据链路层应当有两种不同的协议数据单元，即 LLC 帧和 MAC 帧。从高层来的数据加上 LLC 的帧头就成为 LLC 帧，再向下传送到 MAC 子层，加上 MAC 的帧头和帧尾，组成 MAC 帧。物理层则把 MAC 帧当比特流透明地在数据链路实体间传送。

4.1.2　典型例题分析

例 4-1　在快速以太网物理层标准中，使用两对五类无屏蔽双绞线的是_____。

A. 100Base-TX　　　　B. 100Base-FX

C. 100Base-T4　　　　D. 100Base-T2

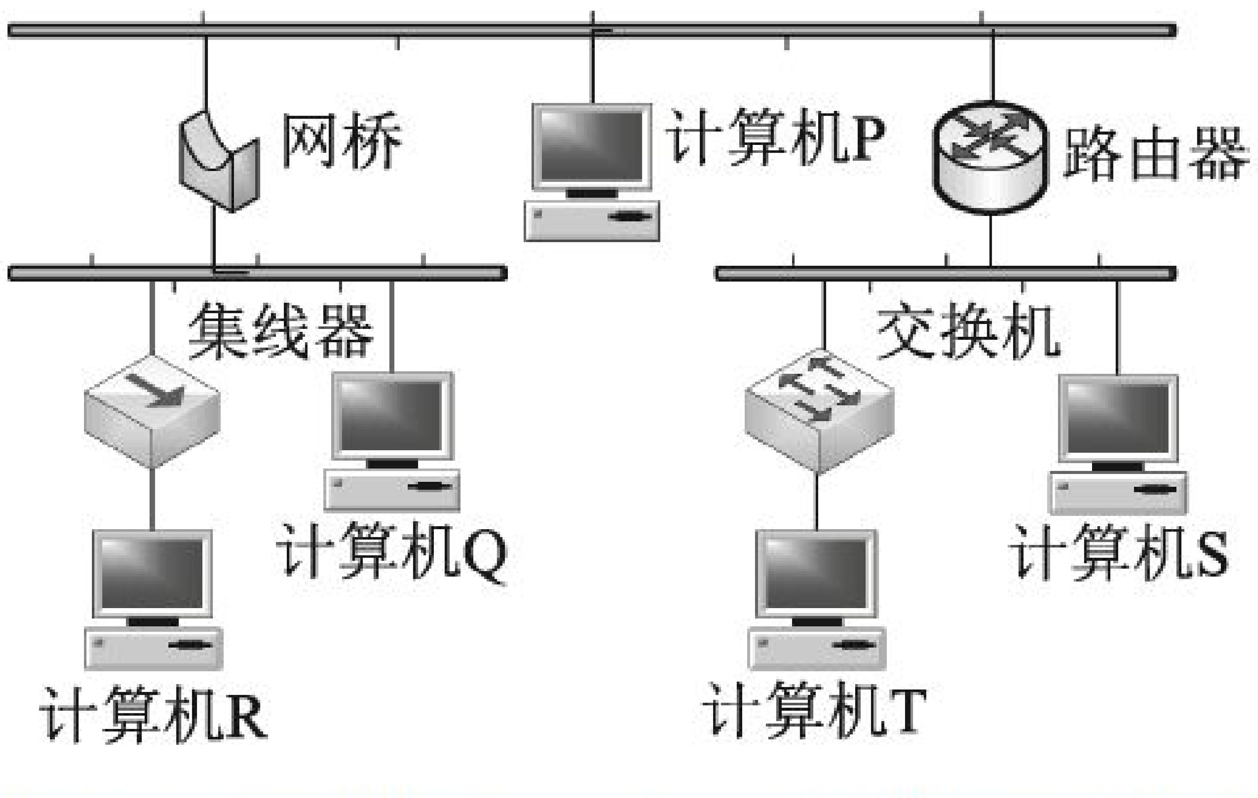
解析：快速以太网使用的传输介质如下表所示。

标　准	传输介质
100Base-T2	两对三类 UTP
100Base-T4	四对三类 UTP
100Base-TX	两对五类 UTP
100Base-FX	一对多模光纤
	一对单模光纤

答案：A

4.1.3　同步练习

某 IP 网络连接如下图所示，在这种配置下，IP 全局广播分组不能够通过的路径是______。



A. 计算机 P 和计算机 Q 之间的路径　　B. 计算机 P 和计算机 S 之间的路径

C. 计算机 Q 和计算机 R 之间的路径　　D. 计算机 S 和计算机 T 之间的路径

4.1.4　同步练习参考答案

B

4.2 逻辑链路控制子层

4.2.1 考点辅导

无论是总线网(CSMA/CD 或令牌总线)还是环型网(令牌环或 FDDI)，相关的标准仅仅定义了对应局域网中的物理层和介质访问控制子层(MAC)或类似层次的协议和规范。

逻辑链路控制子层(LLC)是 ISO OSI/RM 数据链路层(DL)的高子层，其目的是屏蔽不同的介质访问控制方法，以向高层(网络层)提供统一的服务和接口。从总体上来看，LLC 子层的数据传输和处理流程包括接收来自高层实体(网络层实体)的信息，加上 LLC 子层的控制信息，组合成 LLC 帧，并通过 LLC/MAC 的接口，将 LLC 帧填入 MAC 帧中的 DATA 字段，由 MAC 实体负责传递到接收方。接收方的 LLC 实体调用 MAC 层的服务原语，获得对等实体发来的 LLC 帧。LLC 帧的帧格式如图 4-2 所示。

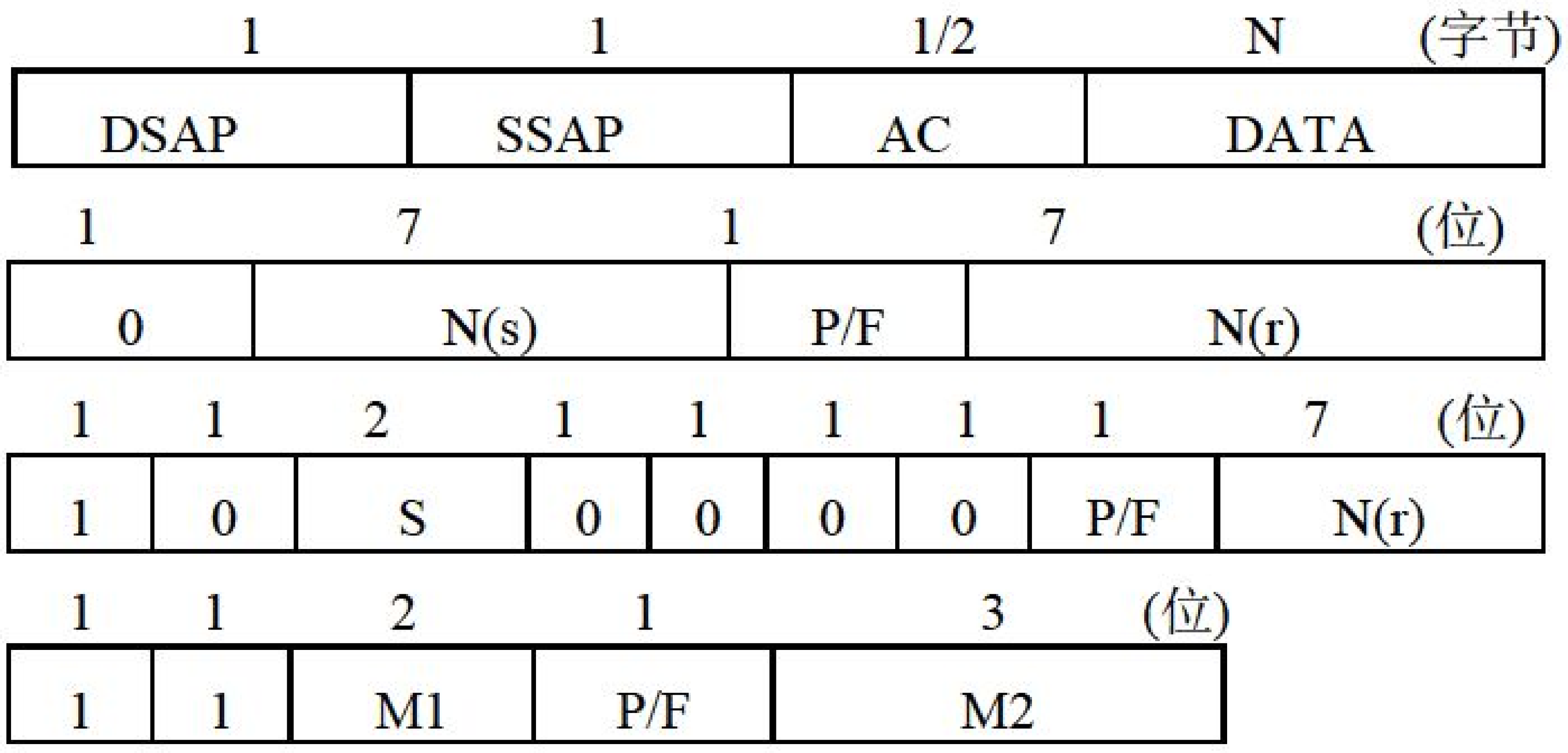


图 4-2　LLC 帧的帧格式

目标/源地址(DSAP/SSAP)各占 1 字节，LLC 地址是一个逻辑地址，用于标识一个高层实体可以访问的端口。DSAP 中的第 1 位为单/组地址标识(I/G)，表示本帧发往某个节点 (由 MAC 帧中的目的地址指定)上的一个或一组端口，后 7 位表示端口号。SSAP 的第 1 位为命令/响应标识(C/R)，表示本帧为命令或者响应帧。

1. LLC 地址

LLC 地址是 LLC 层的服务访问点。IEEE 802 局域网中的地址分两级表示，主机的地址是 MAC 地址。LLC 地址实际上是主机中上层协议实体的地址，一个主机中可以同时有多个上层协议进程，因而就有多个服务访问点。IEEE 802.2 中的地址字段分别用 DSAP 和 SSAP 表示目标地址和源地址，这两个地址都是 7 位长。另外增加的一种功能是可提供组目标地址，而全 1 地址表示所有用户。在源地址字段中的控制位 C/R 用于区分命令帧和响应帧。

2. LLC 服务

LLC 提供以下 3 种服务。

(1) 无确认无连接的服务。这是数据报类型的服务。这种服务因其简单而不涉及任何

流控和差错控制功能，因而也不保证可靠地提交。使用这种服务的设备必须在高层软件中处理可靠性的问题。

(2) 面向连接方式的服务。这种服务类似于 HDLC 提供的服务。在有数据交换的用户之间要建立连接，同时也通过连接提供流控和差错控制功能。

(3) 有确认无连接的服务。这种服务与前面两种服务有所交叉，它提供有确认的数据报，但不建立连接。

3. LLC 协议

LLC 协议与 HDLC 协议兼容，它们之间的区别如下。

(1) LLC 用无编号信息帧支持无连接的服务，称为 LLC1 型操作。

(2) LLC 用 HDLC 的异步平衡方式的操作支持连接方式的 LLC 服务，这种操作称为 LLC2 型操作。LLC 不支持 HDLC 的其他操作。

(3) LLC 用两种新的无编号帧支持有确认无连接的服务，称为 LLC3 型操作。

(4) 通过 LLC 服务访问点支持多路复用，即一对 LLC 实体间可建立多个连接。

4.2.2　典型例题分析

例 4-2　路由器出厂时，默认的串口封装协议是________。(2013 年上半年真题)

A. HDLC　　B. WAP　　C. MPLS　　D. L2TP

解析：路由器默认的串口封装类型是 HDLC，所以一般不用配置 encapsulation hdlc 命令(即设置 HDLC 封装)，默认情况下，路由器会认为串口为 1.544Mb/s 的带宽。

答案：A

例 4-3　IEEE 802 局域网中的地址分为两级，其中 LLC 地址是________。

A. 应用层地址　　B. 上层协议实体的地址

C. 主机的地址　　D. 网卡的地址

解析：由于局域网是分组广播式网络，网络层的路由功能是不需要的，所以在 IEEE 802 标准中，网络层简化成了上层协议的服务访问点(SAP)。又由于局域网使用多种传输介质，而介质访问控制协议与具体的传输介质和拓扑结构有关，所以 IEEE 802 标准把数据链路层划分成了两个子层，与物理介质相关的部分叫作介质访问控制(MAC)子层，与物理介质无关的部分叫作逻辑链路控制(LLC)子层。LLC 子层提供标准的 OSI 数据链路层服务，这使得任何高层协议(如 TCP/IP、SNA 或有关的 OSI 标准)都可以运行于局域网标准之上。

答案：B

4.2.3　同步练习

下列不是 LLC 提供的服务的是________。

A. 无确认无连接的服务　　B. 面向连接方式的服务

C. 有确认无连接的服务　　D. 有确认有连接的服务

4.2.4 同步练习参考答案

D

4.3 IEEE 802.3 标准

4.3.1 考点辅导

4.3.1.1 ALOHA 协议

ALOHA 和它的后继者 CSMA/CD 都是随机访问或竞争发送协议。随机访问意味着对任何站都无法预计其发送的时刻；竞争发送是指所有发送的站自由竞争信道的使用权。

ALOHA 系统是 20 世纪 70 年代美国夏威夷大学的 Norman Abramson(诺曼 •艾布拉姆森)等人为他们的地面无线分组网设计的。这种系统中有多个站共享广播信道。假定所有站的数据业务特征具有明显的突发性，即大部分时间不发送数据，一旦有数据要发送，立即组织成帧以全部信道带宽的速率发送出去。在这种情况下，广播信道由所有站随机地使用，要发送的站不管其他站是否使用信道。可以说信道是完全随机分布控制的。

当然，工作站完全独立而随机地使用信道会发生冲突，只要两个站发送的数据帧在时间上有 1bit 以上的重叠，都会使整个帧出错。幸好，发送站可以通过自发自收校验发现冲突，并随机延迟一段时间后重发冲突帧，如图 4-3 所示。可以看出这种协议的简单性：不需要接收站发回应答，甚至也不需要接收站进行差错校验(假若信道是理想的)。

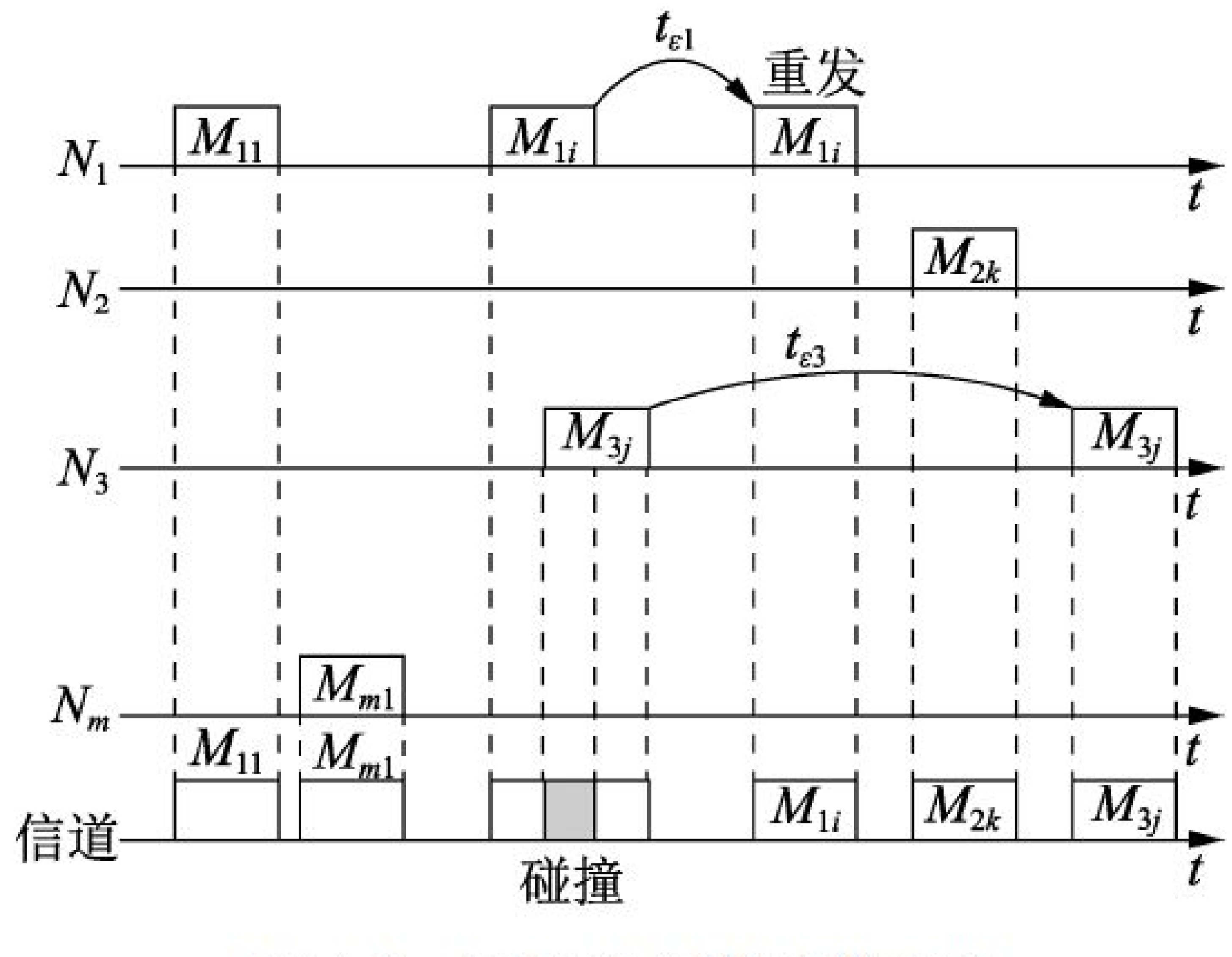


图 4-3 ALOHA 系统工作原理

这种简单系统的实用性取决于其工作效率。下面分析 ALOHA 系统的效率并找出改进的方法。

为了简化讨论，假定：

(1) 无限多个站共享理想的(无差错)广播式信道，这样网络平均负载保持常数。

(2) 所有站发送的帧是等长的，一个帧时为 t_f。

(3) 进入信道的帧数服从泊松分布，每个帧时内产生的帧数加上以前冲突需要重传的帧数之和的平均值为 G(即信道负载)。根据泊松分布，在任一帧时内进入信道的帧数为 K 的概率是

$$P(K)=\frac{G^K \mathrm{e}^{-G}}{K!} \tag{4-1}$$

(4) 在完全随机发送的情况下，一个帧要能发送成功(不冲突)，必须保证在当前帧发送的 t_f 内和当前帧发送之前的区间 t_f 内都没有其他(生成的或重传的)帧进入信道。换言之，冲突区间为 $2t_f$，如图 4-4 所示。

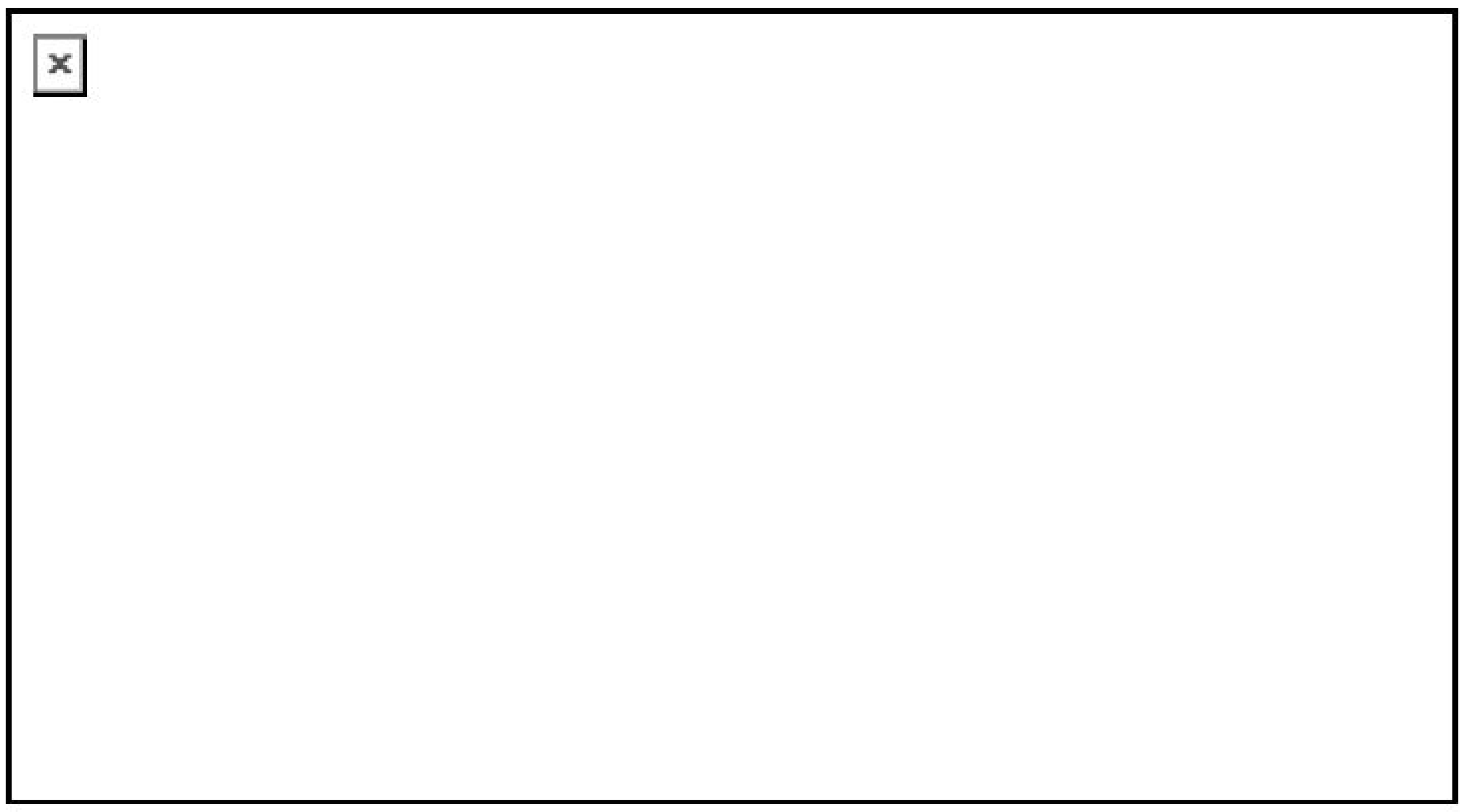


图 4-4　ALOHA 系统的冲突区间

因而在 $2t_f$ 时间内成功发送一帧的概率等于前一个帧时内不发送和后一个帧时内只发送一帧的概率，即

$$P_e = P(0)\times P(1) = G\mathrm{e}^{-2G} \tag{4-2}$$

式(4-2)也表示系统的吞吐率，即单位时间内发送的帧数为

$$S = P_e = G\mathrm{e}^{-2G} \tag{4-3}$$

为了求得最大吞吐率，令 dS/dG=0，从而解得当 G=0.5 时，

$$S_{max} = 1/2\mathrm{e} \approx 0.184 \tag{4-4}$$

1972 年，Robert 发表了一种能把 ALOHA 系统吞吐率提高一倍的方法。他建议把时间划分成离散的时间间隔，每个间隔为 t_f，称为时槽。一个帧无论何时生成，都必须在时槽的起点上发送。这样为了一个帧成功地发送，只需保证在前一个时槽中只有此一个帧生成(或需要重传)，于是冲突区间缩小为 t_f，式(4-2)简化为

$$P_e' = P(1) = G\mathrm{e}^{-G} \tag{4-2$'$}$$

同时有

$$S' = P_e' = G\mathrm{e}^{-G} \tag{4-3$'$}$$

当 G=1 时，得到系统的最大吞吐率

$$S_{max}' = 1/\mathrm{e} \approx 0.368 \tag{4-4$'$}$$

为了区分，通常把这种系统称为分槽的 ALOHA，前一种叫作纯 ALOHA。两种系统效

率(或信道利用率)与负载 G 的关系表示在图 4-5 中。为了进一步提高系统的信道利用率，需增加更多的功能，如载波监听功能，下面详细讨论。

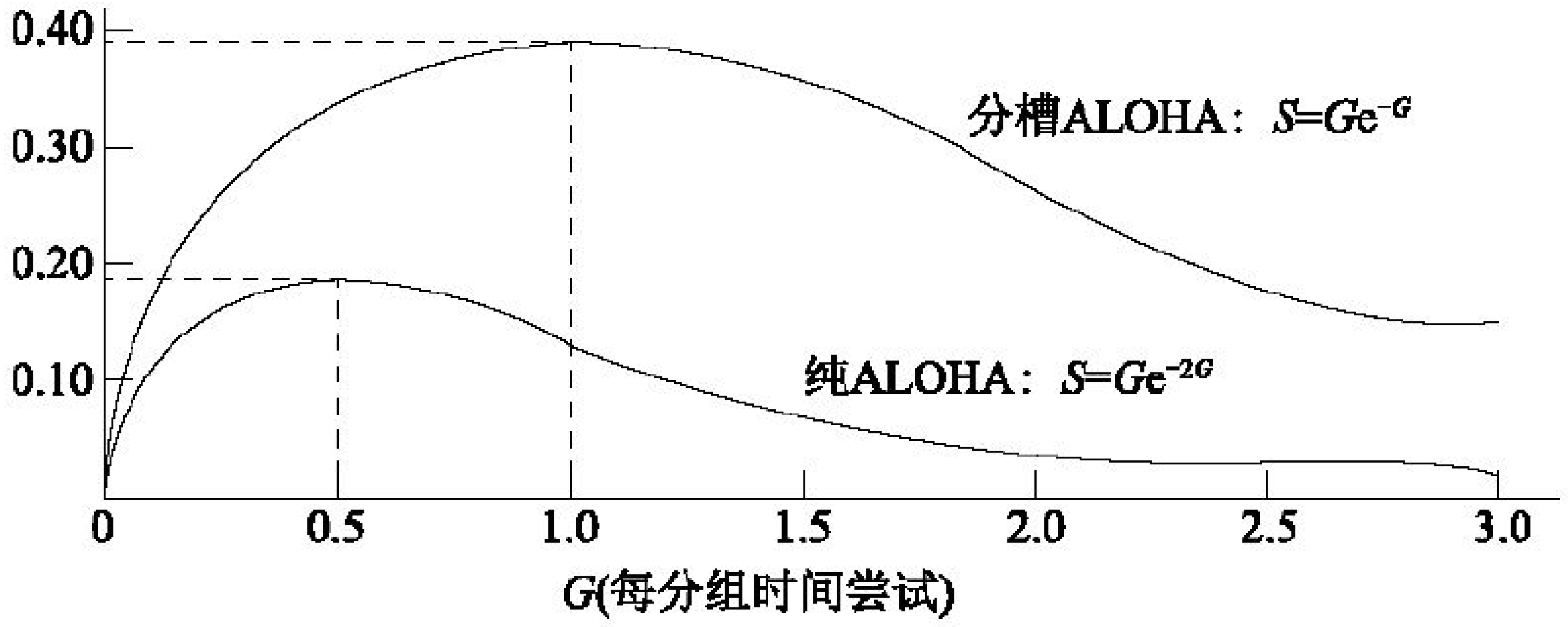


图 4-5　ALOHA 系统中效率与负载的关系

4.3.1.2　CSMA/CD 协议

CSMA/CD 是一种适用于总线结构的分布式介质访问控制方法，是 IEEE 802.3 的核心协议。CSMA 的基本原理是，当一个站在发送数据之前，先监听信道上是否有其他站发送的载波信号，若有，则说明信道正忙；否则信道是空闲的。然后根据预定的策略决定：

- 若信道空闲，是否立即发送。
- 若信道忙，是否继续监听。

1. 监听算法

监听算法并不能完全避免发送冲突，但若对以上两种控制策略进行精心设计，则可以把冲突概率减到最小。据此，有以下 3 种监听算法。

1)　非坚持型监听算法

当一个站准备好帧，发送之前先监听信道：

①　若信道空闲，立即发送；否则转②。

②　若信道忙，等待一个由概率分布决定的随机重发延迟后，重复①。

由于等待了一个由概率分布决定的随机重发延迟，从而减少了冲突的概率；然而，可能出现的问题是因为延迟而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

2)　1-坚持型监听算法

当一个站准备好帧，发送之前先监听信道：

①　若信道空闲，立即发送；否则转②。

②　若信道忙，继续监听，直到信道空闲后立即发送。

这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间；但是多个站同时都在监听信道时必然发生冲突。

3)　P-坚持型监听算法

P-坚持型监听算法吸取了以上两种算法的优点，但较为复杂。

①　若信道空闲，以概率 P 发送，以概率 $(1-P)$ 延迟一个时间单位。一个时间单位等于网络传输时延期 τ 。

②　若信道忙，继续监听，直到信道空闲，转①。

③　若发送延迟一个时间单位 τ，则重复①。

2. 冲突检测(CD)原理

载波监听只能减小冲突的概率，而不能完全避免冲突。当两个帧发生冲突后，若继续发送，将会浪费网络带宽。如果帧比较长，对带宽的浪费就很可观。为了进一步改进带宽的利用率，发送站应采取边发边听的冲突检测方法。具体如下。

①　发送期间同时接收，并把接收的数据与站中存储的数据进行比较。

②　若比较结果一致，说明没有冲突，重复①。

③　若比较结果不一致，说明发生冲突，立即停止发送，并发送一个简短的干扰信号(Jamming)，使所有站都停止发送。

④　发送 Jamming 信号后，等待一段随机长的时间，重新监听，再试着发送。

3. 二进制指数后退算法

按照二进制指数后退算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。随着重发次数 n 的增加，后退时延 t_ζ 的取值范围按 2 的指数增大。即第一次试发时 n 的值为 0，每冲突一次，n 的值加 1，并按式(4-5)计算后退时延，即

$$\begin{cases}\zeta = \text{random}[0,\ 2^n] \\ t_\zeta = \zeta_\tau\end{cases} \tag{4-5}$$

为了避免无限制的重发，要对重发次数 n 进行限制。通常当 n 增加到某一个最大值时停止发送，并向上层协议报告发送错误，等待处理。

4. CSMA/CD 的实现

对于基带总线和宽带总线，CSMA/CD 的实现基本上是相同的，但也有一些差别。

差别一是载波监听的实现。对于基带系统，是检测电压脉冲序列。对于宽带系统，监听站接收 RF 载波以判断信道是否空闲。

差别二是冲突检测的实现。对于基带系统，是把直流电压加到信号上来检测冲突。对于宽带系统，有几种检测冲突的方法。方法之一是把接收的数据与发送的数据逐位比较；另一种方法用于分裂配置，由端头检查是否有破坏了的数据，这种数据的频率与正常数据的频率不同。

4.3.1.3　CSMA/CD 协议的性能分析

吞吐率是单位时间内实际传送的位数。假设网上的站都有数据要发送，没有竞争冲突，各站轮流发送数据，则传送一个长度为 L 的帧的周期为 t_p+t_f。由此可得出最大吞吐率为

$$T = \frac{L}{t_p + t_f} = \frac{L}{d/v + L/R} \tag{4-6}$$

式中：d 为网络段长；v 为信号在铜线中传播的速度(为光速的 65%～77%)；R 为网络提供的数据速率，或称为网络容量。

同时可得出网络利用率为

$$E = \frac{T}{R} = \frac{L/R}{d/v + L/R} = \frac{t_f}{t_p + t_f} \tag{4-7}$$

利用 $a = t_p / t_f$，得

$$E = \frac{1}{a+1} \tag{4-8}$$

a(或者 Rd 的乘积)越大，信道利用率越低。

4.3.1.4 MAC 和 PHY 规范

最早采用 CSMA/CD 协议的网络是 Xerox 公司的以太网。1981 年，DEC、Intel 和 Xerox 3 家公司制定了 DIX 以太网标准。后来，IEEE 802 委员会参考以太网标准制定了局域网标准。以太网是 802.3 标准中的一种。

1. MAC 帧结构

CSMA/CD 方式定义的帧结构内含 8 个字段：前导码(P)、帧起始符(SFD)、目的地址(DA)、源地址(SA)、数据长度(L)、用户数据(DATA)、填充(PAD)和帧校验序列(FCS)。完整的 MAC 帧格式如图 4-6 所示。

7	1	2/6	2/6	2	0～1500	0～46	4	(字节)
P	SFD	DA	SA	L	DATA	PAD	FCS	

图 4-6　CDMA/CD 的 MAC 帧格式

(1) 前导码(P) 字段包含 7 字节，其格式为“1010..1010”。前导码的目的是使接收端进入同步状态，以便数据的接收。

(2) 帧起始符(SFD)占 1 字节(1B)，取值为 10101011。SFD 紧跟在前导码字段之后标识本信息帧的开始。

(3) 目的地址/源地址(DA/SA)各占 2B 或 6B，10Mb/s 的基带网络只使用 6B 地址。目的地址最高位为 0 时表示普通地址，为 1 时表示组地址。全 1 的目的地址是广播地址，所有站都接收这种帧。地址字段的次高位表示采用本地地址或者全局地址，本地地址为两字节(2B)地址，由网络管理员分配；全局地址为 6B 地址，由 IEEE 分配，确保全球唯一。尽管标准中定义的地址字段可以是 2B 或者 6B，但在同一个网络中地址结构应当一致。

(4) 数据长度(L)字段占 2B，表示 DATA 字段的实际长度。

(5) 用户数据(DATA)字段小于 1500B，存放高层 LLC 的信息。

(6) 填充(PAD)字段不大于 46B。为了保证帧发送期间能检测到冲突，IEEE 802.3 规定最小帧为 64B。这个帧长是指从目标地址到校验序列的长度。由于前导码和帧起始符是物理层加上的，因此不包括在帧长中，也不参加帧校验。如果帧的长度不足 64B，要加入最多 46B 的填充位。

(7) 帧校验序列(FCS)占 4B，采用循环冗余校验(CRC)码。

2. CSMA/CD 协议的实现

IEEE 802.3 采用 CSMA/CD 协议，这个协议的载波监听、冲突检测、冲突强化、二进制指数后退等功能都由硬件实现。这些硬逻辑电路包含在网卡中。网卡上的主要器件是以太网数据链路控制器(Ethernet Data Link Controller，EDLC)。这个器件中有两套独立的系统，

分别用于发送和接收。

IEEE 802.3 使用 1-坚持型监听算法，因为这个算法可及时抢占信道，减少空闲期，同时实现也较简单。在监听到网络由活动变到安静后，并不能立即开始发送，还要等待一个最小帧间隔时间，只有在此期间网络持续平静，才能开始试发送。最小帧间隔时间规定为 9.6μs。

在发送过程中继续监听。若检测到冲突，发送 8 个十六进制数的序列 55555555，这就是协议规定的阻塞信号。

接收站要对收到的帧进行校验。除了 CRC 校验外，还要检查帧的长度。短于最小长度的帧被认为是冲突碎片而丢弃，帧长与数据长度不一致的帧以及长度不是整数字节的帧也被丢弃。

3. 物理层规范

表 4-1 所示为 IEEE 802.3 所采用的传输介质(其中的曼码是指曼彻斯特编码)。

表 4-1　IEEE 802.3 的传输介质

项　目	以太网	10Base-5	10Base-2	1Base-5	10Base-T	10Broad-36	10Base-F
拓扑结构	总线型	总线型	总线型	星型	星型	总线型	星型
数据速率/(Mb/s)	10	10	10	1	10	10	10
信号类型	基带 曼码	基带 曼码	基带 曼码	基带 曼码	基带 曼码	宽带 DPSK	基带 曼码
最大段长/m	500	500	200	250	100	360	500，2000
传输介质	粗同轴 电缆	粗同轴 电缆	细同轴 电缆	UTP	UTP	CATV 电缆	光纤

4.3.1.5　交换式以太网

在重负载下，以太网的吞吐率大大下降。实际的通信速率比网络提供的带宽低得多，这是因为所有的站竞争同一信道所引起的。使用交换技术可以改善这种情况，交换式以太网就是 IEEE 802.3 标准的改进。下面简述这种技术的基本原理。

交换式以太网的核心部件是交换机，这种设备有一个高速底板(工作速率为 1Gb/s)。底板上有 4～32 个插槽，每个插槽可连接一块插入卡，卡上有 1～8 个连接器，用于连接带有 10Base-T 网卡的主机。

连接器接收主机发来的帧。插入卡判断目标地址，如果目标站是同一卡上的主机，则把帧转发到相应的连接器端口，否则就转发给高速底板。底板根据专用的协议进一步转发，送达目标站。

当同一插入卡上有两个以上的站发送帧时就发生冲突。分解冲突的方法取决于插入卡的逻辑结构。一种方法是同一卡上的所有端口连接在一起形成一个冲突域，卡上的冲突分解方法与通常的 CSMA/CD 协议一样处理。这样一个卡上同时只能有一个站发送，但整个交换机中有多个插入卡，因而有多个站可同时发送。对整个网络的带宽提高的倍数等于插入卡的数量。

另一种方法是把来自主机的输入由卡上的存储器缓冲，这种设计允许卡上同时有多个端口输入帧。对于存储帧的处理方法仍然是适时转发，这样就不存在冲突了。这种技术可以把标准以太网的带宽提高一或两个数量级。

进一步扩展联网范围的方法是把 10Base-T 的集线器接在交换机上。这样的交换机相当于网桥，它提供采用 10Base-T 技术的局域网之间的互联，并根据目标地址进行帧转发。

4.3.1.6 高速以太网

1. 快速以太网

1995 年，100Mb/s 的快速以太网标准 IEEE 802.3u 正式颁布，这是基于 10Base-T 和 10Base-F 技术、在基本布线系统不变的情况下开发的高速局域网标准。

快速以太网使用的集线器可以是共享型或交换型，也可以通过堆叠多个集线器扩大端口数量。互相连接的集线器起到了中继的作用，扩大了网络的跨距。快速以太网使用的中继器分为两类。Ⅰ类中继器中包含编码/译码功能，它的延迟比Ⅱ类中继器大。

快速以太网的数据速率提高了 10 倍，而最小帧长没变，所以冲突时槽缩小为 4.12μs。以太网计算冲突时槽的公式为

$$\text{slot} \approx 2S/(0.7C) + 2t_{\text{phy}} \tag{4-9}$$

式中，S 为网络的跨距(最长传输距离)；$0.7C$ 为 0.7 倍光速(信号传播速率)；t_{phy} 为发送站物理层时延，由于发送站发送和接收两次，所以取其时延的两倍值。

可得计算快速以太网跨距的计算公式为

$$S \approx 0.35C(L_{\min}/R - 2t_{\text{phy}}) \tag{4-10}$$

2. 千兆以太网

1000Mb/s 以太网的传输速率更快，作为主干网提供无阻塞的数据传输服务。1996 年 3 月，IEEE 成立了 802.3z 工作组，最终制定的 1Gb/s 的以太网标准包括以下内容。

- 1000Base-CX：使用两对 STP 和 9 芯 D 型连接器，最大段长为 25m。
- 1000Base-LX：使用一对 62.5μm 或 50μm 多模光纤，最大段长为 550m；或使用 9μm 的单模光纤，最大段长为 5km。
- 1000Base-SX：使用一对 62.5μm 的多模光纤，最大段长为 550m；或使用一对 50μm 的多模光纤，最大段长为 525m。
- 1000Base-TX：使用一对五类 UTP，最大段长为 100m。

实现 1000Mb/s 的数据速率，需要采用许多新的数据处理技术。首先是最小帧长需要扩展，以便在半双工的情况下增加跨距。另外，802.3z 还定义了一种帧突发方式(Frame Bursting)，使得一个站可以连续发送多个帧。最后物理层编码也采用了与 10Mb/s 不同的编码方式，即 4B/5B 或 8B/9B 编码法。

3. 万兆以太网(10GE)

2002 年 6 月，IEEE 802.3ae 标准发布，支持 10Gb/s 的传输速率。万兆以太网具有以下特点。

- MAC 子层和物理层实现 10Gb/s 的传输速率。
- MAC 子层的帧格式不变，并保留 IEEE 802.3 标准最小和最大帧长度。

- 不支持共享型，只支持全双工，即只可能实现全双工交换型 10Gb/s 以太网。
- 支持星型局域网拓扑结构，采用点到点连接和结构化布线技术。
- 在物理层上分别定义了局域网和广域网两种系列。

不能使用双绞线，只支持多模和单模光纤。

4.3.1.7 虚拟局域网

1. VLAN 的概念

虚拟局域网(Virtual Local Area Network，VLAN)，是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。

VLAN 技术的出现，主要为了解决交换机在进行局域网互联时无法限制广播的问题。这种技术可以把一个 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样广播报文被限制在一个 VLAN 内。

VLAN 是建立在物理网络基础上的一种逻辑子网，因此建立 VLAN 需要相应的支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，需要路由的支持，这时就需要增加路由设备—— 要实现路由功能，既可采用路由器，也可采用 3 层交换机来完成。

2. VLAN 的划分方法

1) 根据端口来划分 VLAN

许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员。被设定的端口都在同一个广播域中。例如，一个交换机的 1～5 端口被定义为虚拟网 AAA，同一交换机的 6～8 端口组成虚拟网 BBB。这样做允许各端口之间的通信，并允许共享型网络的升级。但是，这种划分模式将虚拟网限制在了一台交换机上。

第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN，不同交换机上的若干个端口可以组成同一个虚拟网。

以交换机端口来划分网络成员，其配置过程简单明了。因此，从目前来看，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。

2) 根据 MAC 地址划分 VLAN

根据 MAC 地址划分 VLAN 的方法是根据每个主机的 MAC 地址来划分 VLAN，即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点是，当用户物理位置移动时，即从连接一个交换机换到连接其他交换机时，VLAN 不用重新配置。所以，可认为这种根据 MAC 地址划分的方法是基于用户的 VLAN。这种方法的缺点是，初始化时所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的。而且这种划分的方法也导致交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样 VLAN 就必须不停地配置。

3) 根据网络层划分 VLAN

根据网络层划分 VLAN 的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分 VLAN。虽然这种划分方法是根据网络地址，比如 IP 地址，但它不是路由，与网络

层的路由毫无关系。

这种方法的优点是：用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要；还有，这种方法不需要附加的帧标签来识别 VLAN，这样可以减少网络的通信量。

这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法)，一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，需要更高的技术，同时也更费时。当然，这与各个厂商的实现方法有关。

4) 根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个多播组就是一个 VLAN。根据 IP 组播划分 VLAN 的方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展。当然，这种方法不适合局域网，主要是效率不高。

5) 基于规则的 VLAN

基于规则的 VLAN 也称为基于策略的 VLAN。这是最灵活的 VLAN 划分方法，具有自动配置的能力，能够把相关的用户连成一体，在逻辑划分上称为“关系网络”。网络管理员只需在网管软件中确定划分 VLAN 的规则(或属性)，当一个站点加入网络时，将会被“感知”，并被自动地包含进正确的 VLAN 中。同时，对站点的移动和改变也可自动识别和跟踪。

采用这种方法，整个网络可以非常方便地通过路由器扩展网络规模。有的产品还支持一个端口上的主机分别属于不同的 VLAN，这在交换机与共享式集线器共存的环境中显得尤为重要。自动配置 VLAN 时，交换机中的软件自动检查进入交换机端口的广播信息的 IP 源地址，然后软件自动将这个端口分配给一个由 IP 子网映射成的 VLAN。

3. VLAN 的标准

对 VLAN 的标准，这里只介绍两种比较通用的标准。当然也有一些公司拥有自己的标准，比如 Cisco 公司的 ISL 标准，虽然不是一种大众化的标准，但是由于 Cisco Catalyst 交换机的大量使用，ISL 也成为一种不是标准的标准了。

1) 802.10 VLAN 标准

1995 年，Cisco 公司提倡使用 IEEE 802.10 协议。在此之前，IEEE 802.10 曾经在全球范围内作为 VLAN 安全性的统一规范。Cisco 公司试图采用优化后的 802.10 帧格式在网络上传输 FrameTagging 模式中所必需的 VLAN 标签。然而，大多数 802 委员会的成员都反对推广 802.10。因为，该协议是基于 FrameTagging 方式的。

2) 802.1q

1996 年 3 月，IEEE 802.1 Internetworking(网络互联)委员会结束了对 VLAN 初期标准的修订工作。新出台的标准进一步完善了 VLAN 的体系结构，统一了 FrameTagging 方式中不同厂商的标签格式，并制定了 VLAN 标准在未来一段时间内的发展方向，形成的 802.1q 的标准在业界获得了广泛的推广。它成为 VLAN 史上的一块里程碑。802.1q 的出现打破了虚拟网依赖于单一厂商的僵局，从一个侧面推动了 VLAN 的迅速发展。另外，来自市场的压力使各大网络厂商立刻将新标准融合到他们各自的产品中。

3)　Cisco ISL 标签

ISL(Inter-Switch Link)是 Cisco 公司的专有封装方式，因此只能在 Cisco 的设备上支持。ISL 是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议，通过在交换机直接的端口配置 ISL 封装，即可跨越交换机进行整个网络的 VLAN 分配和配置。

4. VLAN 帧标记

IEEE 802.1q 协议定义了 VLAN 帧标记的格式，在原来的以太帧中增加了 4 字节的帧标记字段，如图 4-7 所示。其中标记控制信息(Tag Control Information，TCI)包括 Priority、CFI 和 VID 3 个部分。

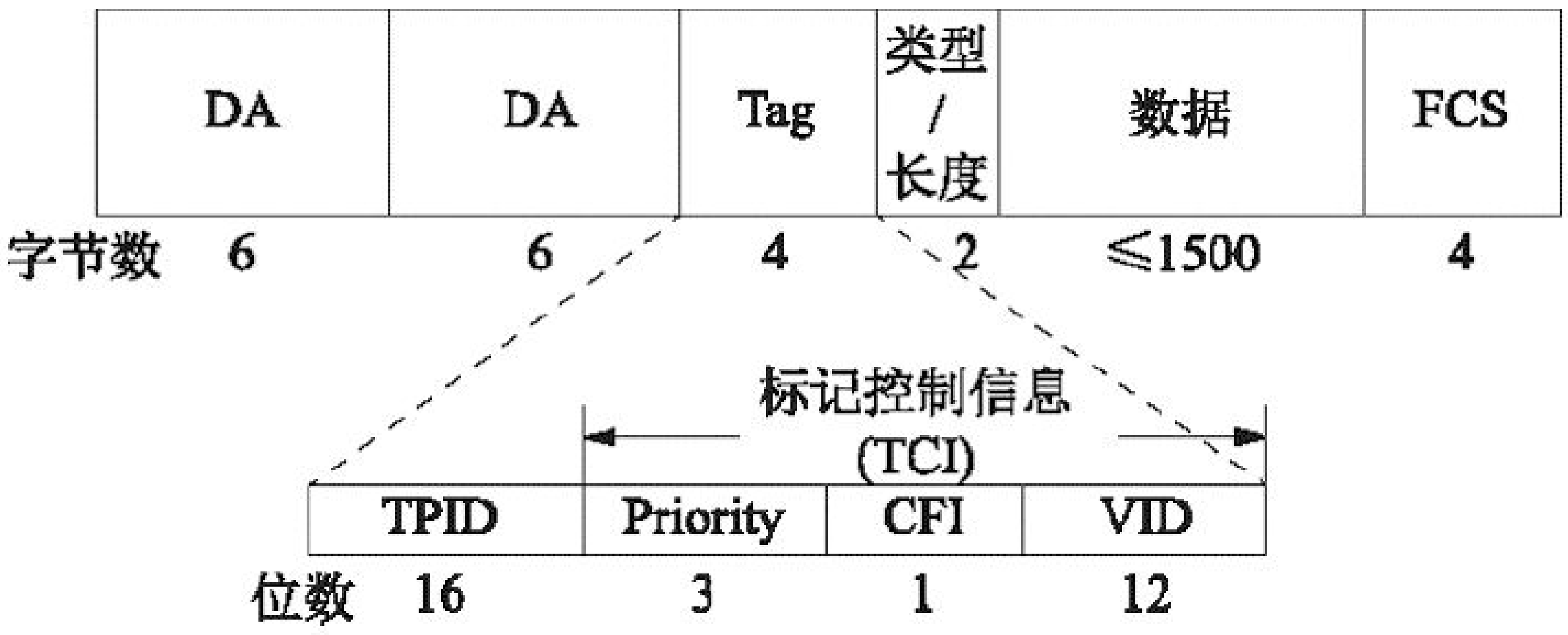


图 4-7　帧格式

- 标记协议标识符(Tag Protocol Identifier，TPID)字段设定为 0x8100，表示该帧包含 802.1q 标记。
- Priority 字段提供了由 802.1q 定义的 8 个优先级。当有多个帧等待发送时，按优先级发送数据包。
- CFI(Canonical Format Indicator，规范格式指示)字段，为 0 表示以太网，为 1 表示 FDDI 和令牌环网。
- VID 字段表示 VLAN 标识符(0～4095)，其中 VID 0 用于识别优先级，VID 4095 保留未用，所以最多可配置 4094 个 VLAN。

5. 虚拟局域网中继

在划分成 VLAN 的交换网络中，交换机端口之间的连接分为两种：接入链路连接(Access-Link Connection)和中继连接(Trunk Connection)。

接入链路只能连接具有标准以太网卡的设备，也只能传送属于单个 VLAN 的数据包。任何连接到接入链路的设备均属于同一广播域。

中继链路是在一条物理连接上生成多个逻辑连接，每个逻辑连接属于一个 VLAN。在进入中继端口时，交换机在数据包中加入 VLAN 标记。这样，在中继链路另一端的交换机就不仅要根据目标地址，而且要根据数据包属于的 VLAN 进行转发决策。

6. VTP 与 VTP 修剪

VLAN 中继协议(VTP)用于在交换网络中简化 VLAN 的管理。VTP 在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管

理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

VTP 有 3 种工作模式：服务器模式、客户模式和透明模式。其中，服务器模式下，可以设置 VLAN 信息，服务器会自动将这些信息广播到网上其他交换机以统一配置；客户模式下，交换机不能配置 VLAN 信息，只能被动接受服务器的 VLAN 配置；透明模式下，可以配置 VLAN 信息，但是不广播自己的 VLAN 信息，同时它可以接收服务器发来的 VLAN 信息后并不使用，而是直接转发给别的交换机。

在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包或者一个未知的单播数据包，交换机都会将其洪泛(Flood)到所有与源 VLAN 端口相关的各个输出端口(包括中继端口)。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动窗口，则这种洪泛发送的数据包是无用的。

为了解决这个问题，可以使用静态或动态的修剪方法。静态修剪就是手工剪掉中继链路上不活动的 VLAN。但是，手工修剪会遇到一些问题，主要是必须根据网络拓扑结构的改变经常重新配置中继链路。在多个交换机组成多个 VLAN 的网络中，这种工作方式很容易出错。

VTP 动态修剪允许交换机之间共享 VLAN 信息，也允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。例如，交换机 A 告诉交换机 B，它有两个活动的 VLAN，即 VLAN1 和 VLAN2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN1，于是，它们就共享这样的事实；VLAN2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。这样做的好处显而易见，如果以后在交换机 B 上添加了 VLAN2 的成员，交换机 B 就会通知交换机 A，它有了一个新的活动的 VLAN2，于是，两个交换机就会动态地把 VLAN2 添加到它们之间的中继链路配置中。

4.3.2 典型例题分析

例 4-4 以下关于 VLAN 标记的说法中，错误的是 (26) 。(2017 年下半年真题 26)

A. 交换机根据目标地址和 VLAN 标记进行转发决策

B. 进入目的网段时，交换机删除 VLAN 标记，恢复原来的帧结构

C. 添加和删除 VLAN 标记的过程处理速度较慢，会引入太大的延迟

D. VLAN 标记对用户是透明的

解析：VLAN 标记只增加了 4 字节，在以太帧之外由硬件芯片完成，速度快，不会引起太大的延迟。

答案：C

例 4-5 以下关于 VLAN 的叙述中，错误的是 (62) 。(2017 年下半年真题 62)

A. VLAN 把交换机划分成多个逻辑上独立的区域

B. VLAN 可以跨越交换机

C. VLAN 只能按交换机端口进行划分

D. VLAN 隔离了广播，可以缩小广播风暴的范围

解析： VLAN 可以根据交换机端口、MAC 地址、网络层以及 IP 组播来划分。

答案： C

例 4-6 VLAN 之间通信需要 (61) 的支持。(2016 年下半年真题 61)

A. 网桥 B. 路由器 C. VLAN 服务器 D. 交换机

解析： 网络中不同的 VLAN 间进行相互通信的时候，需要路由器的支持，实现路由功能，既可采用路由器，也可采用三层交换机来完成。交换机默认为二层交换机。

答案： B

例 4-7 使用 IEEE 802.1q 协议，最多可以配置 (59) 个 VLAN。(2016 年上半年真题 59)

A. 1022 B. 1024 C. 4094 D. 4096

解析： 802.1q 的标志字段占 12 位，支持 4096 VLAN 的识别，但 0 用于识别帧的优先级，4095 作为预留值，故最多可配置 4094 个。

答案： C

例 4-8 VLAN 中继协议(VTP)有不同的工作模式，其中能够对交换机的 VLAN 信息进行添加、删除、修改等操作，并把配置信息广播到其他交换机上的工作模式是 (60) 。(2016 年上半年真题 60)

A. 客户机模式 B. 服务器模式 C. 透明模式 D. 控制模式

解析： VTP 有三种工作模式。

① 服务器模式：可以设置 VLAN 信息，服务器会自动地将这些信息广播到网上的其他交换机，以统一配置。

② 客户模式：交换机不能配置 VLAN 信息，只能被动地接受服务器的 VLAN 配置。

③ 透明模式：可以配置 VLAN 信息，但是不广播自己的 VLAN 信息，同时还可以接收服务器发来的 VLAN 信息后并不使用，而是直接转发给别的交换机。

答案： B

例 4-9 下面关于 VTP 的论述中，错误的是 (61) 。(2016 年上半年真题 61)

A. 静态修剪就是手工剪掉中继链路上不活动的 VLAN

B. 动态修剪使得中继链路上所有共享的 VLAN 都是活动的

C. 静态修剪要求在 VTP 域中的所有交换机都配置成客户机模式

D. 动态修剪要求在 VTP 域中的所有交换机都配置成服务器模式

解析： 所谓静态修剪也叫手工修剪，就是使用如下命令，其格式为 Switch(config-if)#switchport trunk allowed vlan 2，这样其他的 VLAN 就无法进入此交换机，只有用 allowed 参数手工指定的才可以进入该交换机。

动态修剪就是 VTP pruning，即 VTP 的一个功能，它能减少中继链路上不必要的信息量。默认情况下，VLAN 的广播通过中继接口发送到 VLAN 的交换机。

答案： C

例 4-10 以下关于 VLAN 的叙述中，正确的是 (22) 。(2015 年上半年真题 22)

A. VLAN 对分组进行过滤，增强了网络的安全性

B. VLAN 提供了在大型网络中保护 IP 地址的方法

C. VLAN 在可路由的网络中提供了低延迟的互联手段

D. VLAN 简化了在网络中增加、移除和移动主机的操作

解析：VLAN 技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分到不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，因此同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

答案：D

例 4-11 以太网采用物理地址的目的是 __(60)__ 。(2015 年上半年真题 60)

A. 唯一地标识第二层设备

B. 使用不同网络中的设备可以互相通信

C. 用于区分第二层的帧和第三层的分组

D. 物理地址比网络地址的优先级高

解析：MAC(Media Access Control)地址也称为物理地址、硬件地址，用来定义网络设备的位置。在 OSI 模型中，第三层网络层负责 IP 地址，第二层数据链路层则负责 MAC 地址。

答案：A

4.3.3 同步练习

1. 在局域网中可动态或静态划分 VLAN，静态划分 VLAN 是根据____划分。

   A. MAC 地址　B. IP 地址　C. 端口号　D. 管理区域

2. 动态划分 VLAN 的方法中不包括____。

   A. 网络层协议　B. 网络层地址　C. 交换机端口　D. MAC 地址

3. 在局域网中划分 VLAN，不同 VLAN 之间必须通过 (1) 才能互相通信，属于各个 VLAN 的数据帧必须打上不同的 (2) 。

   (1) A. 中继端口　B. 动态端口　C. 接入端口　D. 静态端口

   (2) A. VLAN 优先级　B. VLAN 标记　C. 用户标识　D. 用户密钥

4. 以太网帧格式如下图所示，其中的“长度”字段的作用是______。

前导字符	帧起始符	目的地址	源地址	长度	数据	填充	校验和

   A. 表示数据字段的长度

   B. 表示封装的上层协议的类型

   C. 表示整个帧的长度

   D. 既可以表示数据字段的长度，也可以表示上层协议的类型

5. IEEE 802.3 规定的最小帧长为 64B，这个帧长是指________。

   A. 从前导字段到校验和的字段　B. 从目标地址到校验和的长度

   C. 从帧起始符到校验和的长度　D. 数据字段的长度

6. 下面列出的 4 种快速以太网物理层标准中，使用两对五类无屏蔽双绞线作为传输介

质的是______。

A. 100Base-FX　　B. 100Base-T4

C. 100Base-TX　　D. 100Base-T2

7. 千兆以太网标准 802.3z 定义了一种帧突发方式(Frame Bursting)，这种方式是指________。

A. 一个站可以突然发送一个帧

B. 一个站可以不经过竞争就启动发送过程

C. 一个站可以连续发送多个帧

D. 一个站可以随机地发送紧急数据

8. 在交换机之间的链路中，能够传送多个 VLAN 数据包的是______。

A. 中继连接　　B. 接入链路　　C. 控制连接　　D. 分支链路

9. 要实现 VTP 动态修剪，在 VTP 域中的所有交换机都必须配置成_______。

A. 服务器　　B. 服务器或客户机　　C. 透明模式　　D. 客户机

10. 按照 Cisco 公司的 VLAN 中继协议(VTP)，当交换机处于______模式时可以改变 VLAN 配置，并把配置信息分发到管理域中的所有交换机。

A. 客户机(Client)　　B. 传输(Transmission)

C. 服务器(Server)　　D. 透明(Transparent)

11. IEEE 802.1q 协议的作用是______。

A. 生成树协议　　B. 以太网流量控制

C. 生成 VLAN 标记　　D. 基于端口的认证

12. CSMA/CD 协议可以利用多种监听算法来减小发送冲突的概率，下面关于各种监听算法的描述中，正确的是______。

A. 非坚持型监听算法有利于减少网络空闲时间

B. 坚持型监听算法有利于减少冲突的概率

C. 坚持型监听算法无法减少网络的空闲时间

D. 坚持型监听算法能够及时抢占信道

13. IEEE 802.11 采用了类似于 802.3 CSMA/CD 协议的 CSMA/CA 协议，之所以不采用 CSMA/CD 协议的原因是______。

A. CSMA/CA 协议的效率更高　　B. CSMA/CD 协议的开销更大

C. 为了解决隐蔽终端问题　　D. 为了引进其他业务

14. VLAN 中继协议(VTP)用于在大型交换网络中简化 VLAN 的管理。按照 VTP 协议，交换机的运行模式分为 3 种：服务器模式、客户机模式和透明模式。下面关于 VTP 协议的描述中，错误的是_____ 。

A. 交换机在服务器模式下能创建、添加、删除和修改 VLAN 配置

B. 一个管理域中只能有一个服务器

C. 在透明模式下可以进行 VLAN 配置，但不能向其他交换机传播配置信息

D. 交换机在客户机模式下不允许创建、修改或删除 VLAN

15. 在生成树协议(STP)IEEE 802.1d 中，根据______来选择根交换机。

A. 最小的 MAC 地址　　B. 最大的 MAC 地址

C. 最小的交换机 ID　　D. 最大的交换机 ID

16. 在快速以太网物理层标准中，使用两对五类非屏蔽双绞线的是_____。

A. 100Base-TX　　B. 100Base-FX

C. 100Base-T4　　D. 100Base-T2

17. 关于 IEEE 802.3 的 CSMA/CD 协议，下面结论中错误的是______。

A. CSMA/CD 是一种解决访问冲突的协议

B. CSMA/CD 协议适用于所有 802.3 以太网

C. 在网络负载较小时，CSMA/CD 协议的通信效率很高

D. 这种网络协议适合传播非实时数据

18. 以下关于 IEEE 802.3ae 标准的描述中，错误的是______。

A. 支持 802.3 标准中定义的最小和最大帧长

B. 支持 IEEE 802.3ad 链路汇聚协议

C. 使用 1310nm 单模光纤作为传输介质，最大段长可达 10km

D. 使用 850nm 多模光纤作为传输介质，最大段长可达 10km

19. 以太网的 CSMA/CD 协议采用坚持型监听算法。与其他监听算法相比，这种算法的主要特点是______。

A. 传输介质利用率低，冲突概率也低

B. 传输介质利用率高，冲突概率也高

C. 传输介质利用率低，但冲突概率高

D. 传输介质利用率高，但冲突概率低

20. 快速以太网物理层规范 100Base-TX 规定使用______。

A. 一对五类 UTP，支持 10Mbps/100Mbps 自动协商

B. 一对五类 UTP，不支持 10Mbps/100Mbps 自动协商

C. 两对五类 UTP，支持 10Mbps/100Mbps 自动协商

D. 两对五类 UTP，不支持 10Mbps/100Mbps 自动协商

21. 通过交换机连接的一组工作站______。

A. 组成一个冲突域，但不是一个广播域　　B. 组成一个广播域，但不是一个冲突域

C. 既是一个冲突域，又是一个广播域　　D. 既不是冲突域，也不是广播域

22. 利用交换机可以把网络划分成多个虚拟局域网(VLAN)。一般情况下，交换机默认的 VLAN 是______。

A. VLAN0　　B. VLAN1　　C. VLAN10　　D. VLAN1024

23. 当启动 VTP 修剪功能后，如果交换端口中加入一个新的 VLAN，则立即______。

A. 剪断与周边交换机的连接

B. 把新的 VLAN 中的数据发送给周边交换机

C. 向周边交换机发送 VTP 连接报文

D. 要求周边交换机建立同样的 VLAN

4.3.4　同步练习参考答案

1. C	2. C	3.(1) A　(2) B	4. D	5. B	6. C	7. C	8. A
9. B	10. C	11. C	12. D	13. C	14. B	15. C	16. A
17. B	18. D	19. B	20. C	21. B	22. B	23. C	

4.4　局域网互联

4.4.1　考点辅导

局域网用网桥互联，IEEE 802 标准中包含两种关于网桥的规范，即透明网桥和源路由网桥。

1. 网桥协议的体系结构

在 IEEE 802 体系结构中，站地址是由 MAC 子层协议说明的，网桥在 MAC 子层起中继作用。网桥可以直接连接两个局域网，此时这两个局域网运行相同的 MAC 和 LLC(逻辑链路控制)协议；如果两个局域网相距较远，也可以用两个网桥分别连接一个局域网，两个网桥之间再用通信线路相连(可以是其他网络)。

一个网桥可以连接多个局域网，但网桥连接的局域网多于两个时，网桥必须具有路由选择的功能。为了对网桥的路由选择提供支持，MAC 层地址应当分为两部分：网络地址部分(标识互联网中唯一的局域网)和站地址部分(标识某个局域网中唯一的工作站)。IEEE 802.5 标准建议：16 位 MAC 地址分成 7 位的局域网地址和 8 位的工作站地址，48 位的 MAC 地址分成 14 位的局域网地址和 32 位的工作站地址，其余的位用于区分组地址/单地址以及局部地址/全局地址。

2. 生成树网桥

生成树网桥是一种透明网桥，这个网桥插入电缆后就可自动完成路由选择的功能，无须由用户装入路由表或设置参数，桥内部动态地维护地址映射表，根据该地址映射表，网桥决定收到的帧被转发到对应的子网，或者通过该子网作进一步的转发。

这种网桥的原理很简单：当网桥收到每一个帧时，都执行地址表扩充和帧转发两项工作。地址表扩充是从帧中取出信源节点地址，并填写地址表，从而使网桥“了解”哪些节点属于哪个子网。帧转发是网桥根据帧中的信宿节点地址，查找地址表，如果表中有对应的地址，帧被转发到指定的网络；否则，转发给本网桥连接的所有子网(广播)。

此类网桥得以实现的关键是假定任意两个局域网之间只有一条唯一的通路。当增加冗余的网桥时，如不采取别的措施，会出现环路问题。解决这个问题的措施是构造基于网桥的支撑树(生成树)。构造支撑树的目的是在增加冗余设备提高网络可靠性的同时，也解决网络循环连接带来的问题。

构造支撑树的基本思想是，首先选择网络中的某个网桥(一般选择位置处于相对中心的

网桥)作为树的根，然后从与该树(最初只有根)相邻(可以通过某个子网直接访问)的网桥集合中选择一个加入支撑树，选择的条件是加入该网桥不会形成环路。这种选择的过程继续进行，直至支撑树可以互联所有的子网，剩下的网桥留作备用。

3. 源路由网桥

源路由网桥的核心思想是，由帧的发送者显式地指明路由信息(RI)。RI 由网桥地址和局域网标识符的序列组成，包含在帧头中。每个收到帧的网桥根据帧头中的地址信息可以知道自己是否在转发路径中，并可以确定转发的方向。

确定路径的基本思想是，如果源节点不知道路径，则发送一个具有测试功能的广播帧，广播帧被每个网桥接收。接到广播帧的网桥检查广播帧中的 RI 字段，如果本网桥号已经在 RI 中，不做任何处理；否则，向 RI 中增加段号，并将该帧转发到与之连接且网号未在帧中出现的其他子网。当信宿节点接到该测试帧后，向源节点返回一个应答帧。应答帧中包含了所需的路径信息，并沿着测试帧途经的路径反向传递。由于广播的缘故，源节点会收到多个应答帧，通过某种算法从中选择一条路径。

源路由网桥的优点是可以获得最佳路径；缺点是测试帧可能会形成“广播风暴”。

4.4.2 典型例题分析

例 4-12 某 STP 网络从链路故障中恢复时，端口收敛时间超过 30s，处理该故障的思路不包括__(70)__。(2017 年下半年真题 70)

A. 确认对端端口开启 STP　　B. 确认端口是工作在 STP 模式

C. 确认端口的链路类型是点对点　　D. 确认端口模式为中继模式

解析： STP 的网络拓扑中出现链路故障或链路故障恢复后，业务流量恢复需要超过 30 秒，即端口无法快速收敛，此时需要检查：①确认对端端口是否开启 STP；②检查端口是否工作在 STP 模式；③检查端口的链路类型是否为点对点。

答案： D

例 4-13 STP 协议的作用是__(60)__。(2016 年下半年真题 60)

A. 防止二层环路　　B. 以太网流量控制

C. 划分逻辑网络　　D. 基于端口的认证

解析： STP 协议的作用是防止二层环路，通过阻塞部分端口，将网络修剪成树形结构。一般来说，产生交换环路会造成广播风暴，使交换机处于忙碌状态，阻塞正常的网络流量，还会造成 MAC 地址表不稳定，而利用 STP 协议正好可以解决这个问题。

答案： A

例 4-14 网桥怎样知道网络端口连接了哪些网站？__(63)__当网桥连接的局域网出现环路时怎么办？__(64)__(2016 年下半年真题 63、64)

(63) A. 如果从端口收到一个数据帧，则将其目标地址记入该端口的数据库

B. 如果从端口收到一个数据帧，则将其源地址记入该端口的数据库

C. 向端口连接的各个站点发送请求以便获取其 MAC 地址

D. 由网络管理员预先配置好各个端口的地址数据库

(64) A. 运行生成树协议阻塞一部分端口

B. 运行生态主机配置协议重新分配端口地址

C. 通过站点之间的协商产生一部分备用端口

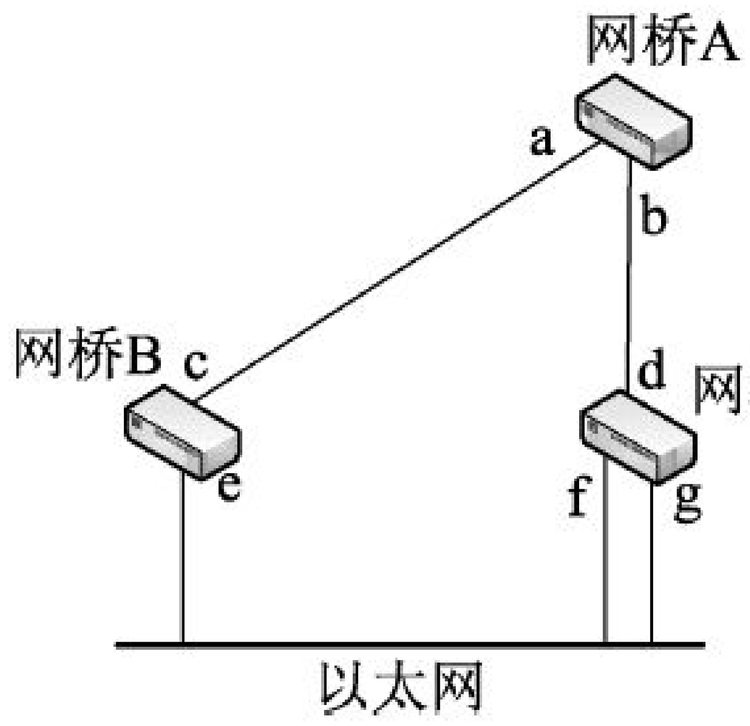
D. 各个网桥通过选举产生多个没有环路的生成树

解析：网桥查看每个端口出现的帧，将其源地址记入该端口的数据库，这样就可以了解各个端口连接了哪些网站。当网桥连接的局域网出现环路时，所有的网桥通过运行生成树协议，阻塞一部分端口，使得不再出现环路。

STP 协议的作用是防止二层环路，通过阻塞部分端口，将网络修剪成树形结构。

答案：(63) B (64) A

例 4-15 如下图所示，网桥 A、B、C 连接多个以太网。已知网桥 A 为根网桥，各个网桥的 a、b、f 端口为指定端口。那么按照快速生成树协议标准 IEEE 802.1d-2004，网桥 B 的 c 端口为 (63) 。(2016 年上半年真题 63)



A. 根端口(Root Port)　　B. 指定端口(Designated Port)

C. 备份端口(Backup Port)　　D. 替代端口(Alternate Port)

解析：根网桥为 A，那么网桥的 a、b 端口都是指定端口，与 STP 协议一样，每个以太网网桥段内必须有一个指定端口，题意中网桥 C 的 f 端口为指定端口。

替换端口：当一个端口收到了来自非自身的 BPDU，并且这个 BPDU 的优先级只比指定端口接收到的低，那么这个端口就会转变为替换端口，作为通往网桥的替代路径，一旦指定端口的路线失效，该条替换的路径将立即使用，对于 SW2 来说，e 端口就是替换端口。

备份端口：指定端口的备份端口，作为通往某网段的备用路径，其实就是在共享网络中，才可能出现备份端口，因为在那种网络中交换机才可能出现到同一个网络的冗余线路，也就是本题中网桥 C 的 g 端口。

答案：A

例 4-16 根据 STP 协议，网桥 ID 最小的交换机被选举为根网桥，网桥 ID 由 (12) 字节的优先级和 6 字节的 (13) 组成。(2015 年下半年真题 12、13)

(12) A. 2　　B. 4　　C. 6　　D. 8

(13) A. 用户标识　　B. MAC 地址　　C. IP 地址　　D. 端口号

解析：网桥 ID 由交换机优先级(用 2 字节表示，默认是 32 768，最小的是 4096，其他的都是 4096 的倍数)和 MAC 地址(6 字节)组成。交换机的每个接口有一个 MAC 地址。

答案：(12) A　(13) B

例 4-17 当局域网中更换交换机时，怎样保证新交换机成为网络中的根交换机？ (23) (2015 年上半年真题 23)

A. 降低网桥优先级　　B. 改变交换机的 MAC 地址

C. 降低交换机端口的根通路费用　　D. 为交换机指定特定的 IP 地址

解析：生成树协议根据网桥 ID 选择根交换机，网桥 ID 最小的交换机将被选为根网桥。网桥 ID 由网桥优先级和网桥 MAC 地址两部分组成，如果交换机的优先级相同，则比较其 MAC 地址，地址值越小，其就被选举为根网桥。

答案：A

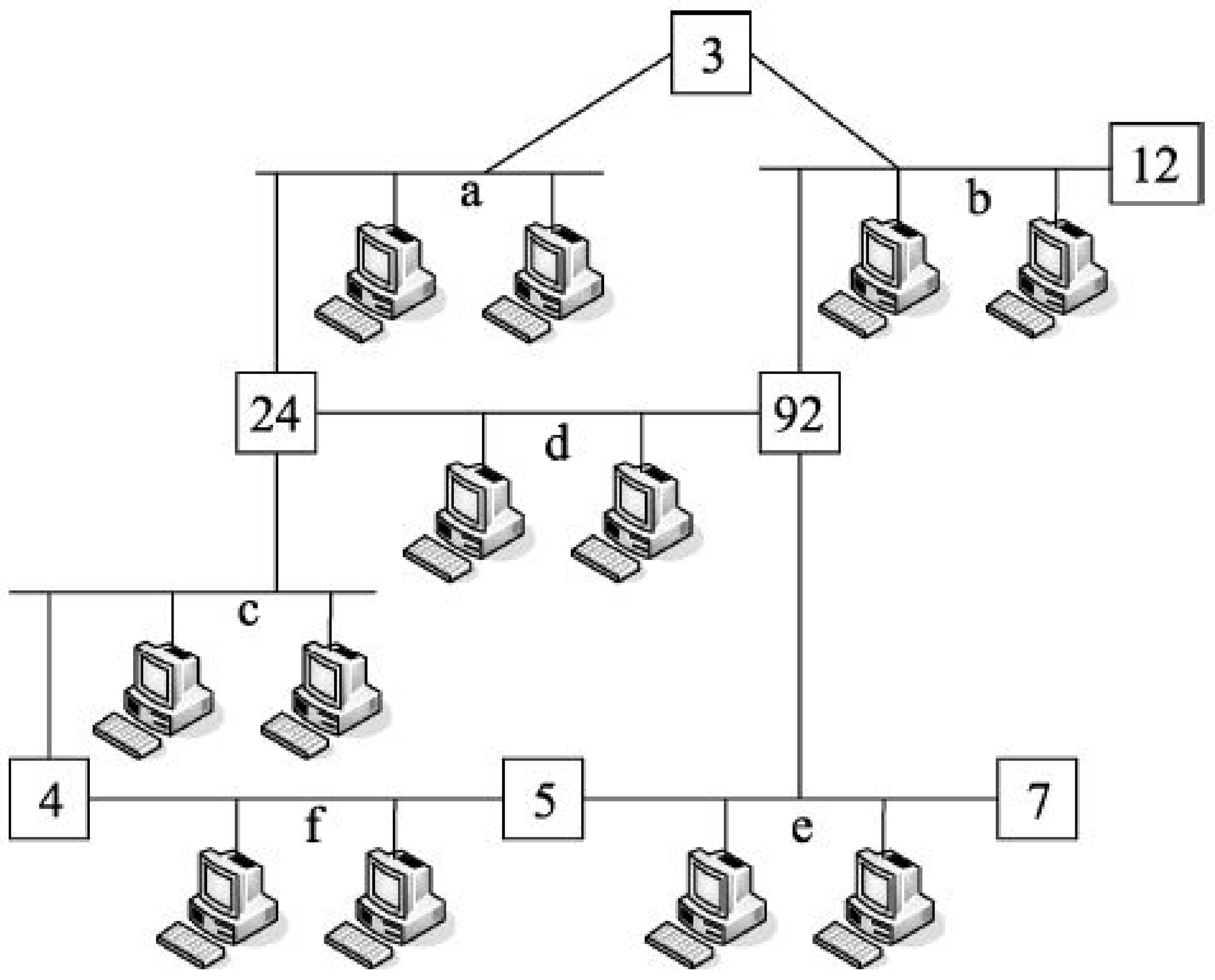
4.4.3 同步练习

1. 按照 IEEE 802.1d 协议，当交换机端口处于________状态时，既可以学习 MAC 帧中的源地址，又可以把接收到的 MAC 帧转发到适当的端口。

A. 阻塞(Blocking)　　B. 学习(Learning)

C. 转发(Forwarding)　　D. 监听(Listening)

2. 下图表示一个局域网的互联拓扑，方框中的数字是网桥 ID，用字母来区分不同的网段。按照 IEEE 802.1d 协议，ID 为 (1) 的网桥被选为根网桥，如果所有网段的传输费用为 1，则 ID 为 92 的网桥连接网段 (2) 的端口为根端口。



(1) A. 3　　B. 7　　C. 92　　D. 12

(2) A. a　　B. b　　C. d　　D. e

4.4.4 同步练习参考答案

1. C　 2. (1) A　(2) B

4.5 城　域　网

4.5.1 考点辅导

4.5.1.1 城域以太网

1. 城域以太网论坛

城域以太网论坛(MEF)是由网络设备制造商和网络设备运营商组成的非营利性组织，专

门从事城域以太网的标准化工作。MEF 的承载以太网(Carrier Ethernet)技术规范提出了以下几种业务类型。

(1) 以太网专用线(EPL)。

(2) 以太网虚拟专线(EVPL)：在一对用户以太网之间通过第三层技术提供点对点的虚拟以太网连接。

(3) 以太局域网服务(E-LAN Services)。

2. E-LAN 服务

提供 E-LAN 服务的基本技术是 802.1q 的 VLAN 帧标记。这种技术定义在 IEEE 802.1ad 的运营商网桥协议(Provider Bridge Protocol)中，被称为 Q-in-Q 技术。

3. 802.1ah 标准

Q-in-Q 实际上是把用户 VLAN 嵌套在城域以太网的 VLAN 中传送，所有用户的 MAC 地址在城域以太网中都是可见的，这使得网络安全受到威胁。因此 IEEE 802.1ah 标准提出了运营商主干网桥(PBB)协议。

4.5.1.2　弹性分组环

弹性分组环(Resilient Packet Ring，RPR)是一种采用环型拓扑的城域网技术。2004 年公布的 IEEE 802.17 标准定义了 RPR 的介质访问控制方法、物理层接口及层管理参数，并提出了用于环路检测和配置、失效恢复及带宽管理的一系列协议。RPR 支持的数据速率可以达到 10Gb/s。

1. 体系结构

RPR 的体系结构如图 4-8 所示。RPR 采用了双环结构，由内层的环 1 和外层的环 0 组成，每个环都是单方向传送。相邻工作站之间的跨距包含传送方向相反的两条链路。RPR 支持多达 255 个工作站，最大环周长为 2000km。

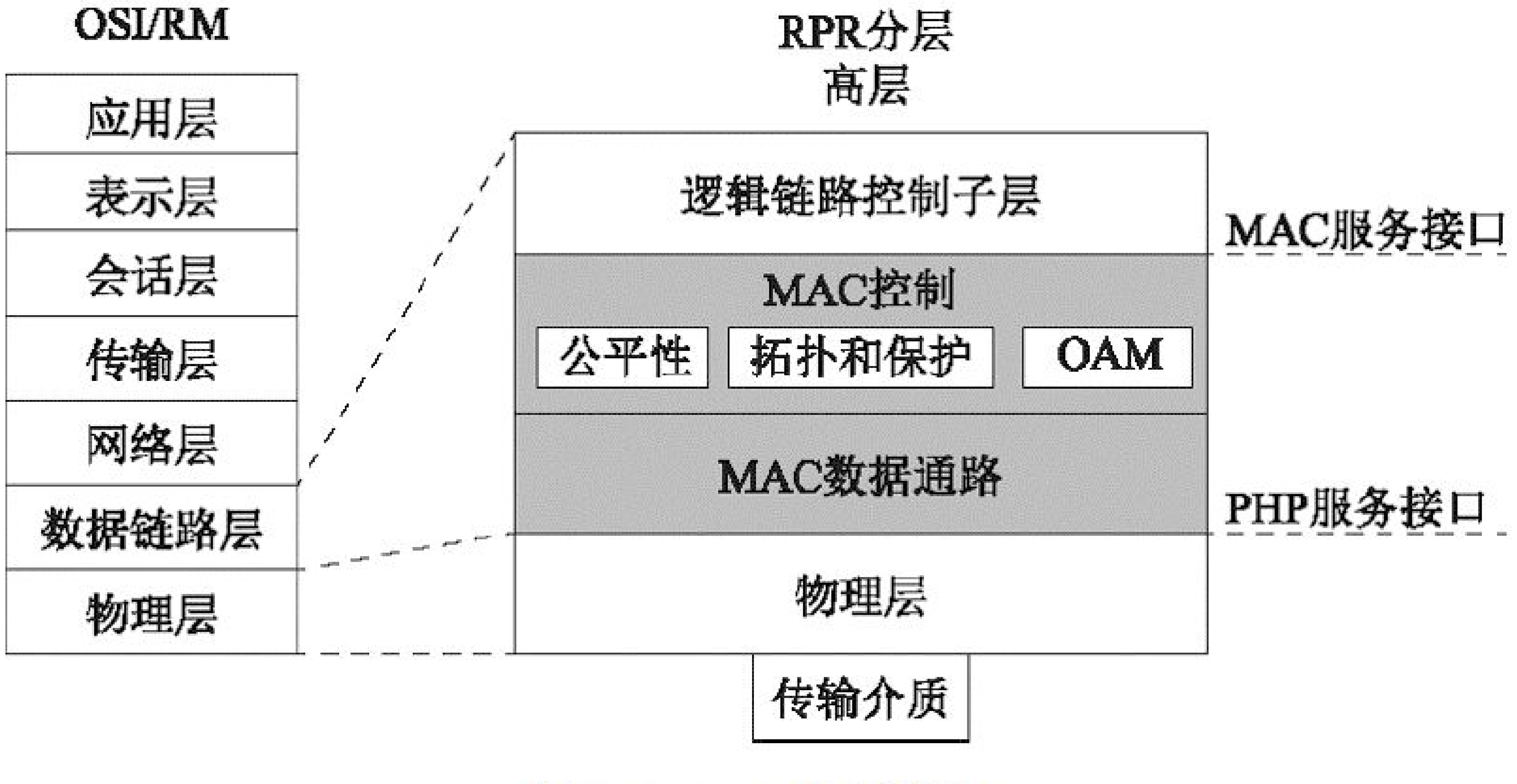


图 4-8　RPR 体系结构

2. RPR 的关键技术

RPR 的关键技术有业务类型、空间复用、拓扑发现、公平算法和环自愈保护。

4.5.2 典型例题分析

例 4-18 城域以太网在各个用户以太网之间建立多点第二层连接，IEEE 802.1ah 定义的运营商主干网协议提供的基本技术是在用户以太帧中再封装一层 __(26)__，这种技术被称为 __(27)__ 技术。(2014 年下半年真题 26、27)

(26) A. 运营商的 MAC 帧头　　B. 运营商的 VLAN 标记
C. 用户 VLAN 标记　　D. 用户帧类型标记

(27) A. Q-in-Q　　B. IP-in-IP　　C. NAT-in-NAT　　D. MAC-in-MAC

解析：MAC-in-MAC 封装又称网络提供商骨干桥(PBB)技术，遵循 IEEE 802.1ah 标准。其基本思路是将用户的以太网数据帧再封装一个运营商的以太网帧头，形成两个 MAC 地址。

答案：(26) A　(27) D

例 4-19 RPR 支持的数据速率可以达到________。

A. 10Gb/s　　B. 12Gb/s　　C. 15Gb/s　　D. 16Gb/s

解析：RPR 支持的数据速率可以达到 10Gb/s。

答案：A

4.5.3 同步练习

下列不是 RPR 的关键技术的是________。

A. 业务类型　　B. 空间复用　　C. 环自愈保护　　D. 时间复用

4.5.4 同步练习参考答案

D

4.6 本 章 小 结

本章知识点在 2009 年的新大纲中将本章节中原有的无线局域网部分，单独列成了一个新的章节——无线通信网。

本章主要要求考生掌握局域网和城域网技术，包括 IEEE 体系结构、以太网、网络连接设备、高速 LAN 技术、VLAN、CSMA/CA。其中以太网以及 VLAN 是考试重点。

本章相关知识点在历次考试中分布相对集中，分值在 8 分左右，是考试的重点。本章前几节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

4.7 达标训练题及参考答案

4.7.1 达标训练题

1. 下面的消除交换机上 MAC 地址漂移告警的方法中，描述正确的是__(68)__。

① 人工把发生漂移的接口 shutdown

② 在接口上配置 error-down，自动 down 掉漂移的端口

③ 在接口上配置 quit-vlan，使发生漂移的接口从指定 VLAN 域内退出

④ 在接口上配置 stp tc-protection，解决 MAC 地址漂移问题

A. ①②③④　　B. ②③④　　C. ②③　　D. ①②③

2. 1996 年 3 月，IEEE 成立了 802.3z 工作组，开始制定 1000Mb/s 标准。下列千兆以太网中不属于该标准的是__(19)__。

A. 1000Base-SX　　B. 1000Base-LX

C. 1000Base-T　　D. 1000Base-CX

3. IEEE 802.3ae 10Gb/s 以太网标准支持的工作模式是______。

A. 单工　　B. 半双工　　C. 全双工　　D. 全双工和半双工

4. 采用 10Base-5 的局域网表示__(1)__。采用特性阻抗为__(2)__Ω的粗同轴电缆。这种网络的收发器不在网卡上，而是直接与电缆相连，收发器电缆最长为__(3)__，最大节点数限于__(4)__个工作站。

(1) A. 数据传输速率为 10Mb/s 的基带传输网络，最大段长为 500m

B. 数据传输速率为 100Mb/s 的基带传输网络，最大段长为 500m

C. 数据传输速率为 10kb/s 的基带传输网络，最大段长为 200m

D. 数据传输速率为 10Mb/s 的宽带传输网络，最大段长为 500m

(2) A. 20　　B. 30　　C. 50　　D. 75

(3) A. 10　　B. 15　　C. 20　　D. 25

(4) A. 50　　B. 100　　C. 150　　D. 200

5. 局域网参考模型中，两个子系统的同等实体按照协议进行通信，在一个系统中，上下层之间则通过接口进行通信，用______来定义接口。

A. 服务访问点　　B. 服务原语　　C. 服务数据单元　　D. 协议数据单元

6. 决定局域网特性的主要技术要素是网络拓扑、传输介质和______。

A. 数据库软件　　B. 网络操作系统

C. 体系结构　　D. 介质访问控制协议

7. 以太网中，当数据传输速率提高时，帧的发送时间要按比例缩短，这样有可能会影响冲突的检测。为了能有效地检测冲突，可以__(1)__或者__(2)__。快速以太网仍然遵循 CSMA/CD，它采取__(3)__而将最大电缆长度减少到 100m 的方式，使以太网的数据传输速率提高到 100Mb/s。为了支持不同的传输介质，快速以太网提供了 3 种技术标准，即 100Base-T4、100Base-TX 和 100Base-FX，其中 100Base-T4 使用__(4)__。

(1) A. 减小电缆介质的长度　　B. 增加电缆介质的长度
C. 降低电缆介质的损耗　　D. 提高电缆介质的导电率

(2) A. 减小最短帧长　　B. 增大最短帧长
C. 减小最大帧长　　D. 增大最大帧长

(3) A. 改变最短帧长　　B. 改变最大帧长
C. 保持最短帧长不变　　D. 保持最大帧长不变

(4) A. 4 对三类线　　B. 2 对三类线
C. 4 对五类线　　D. 2 对五类线

8. 在局域网中，以下______传输介质既可以用于物理层 10Base-T 协议，又可以用于 100Base-T 协议。

A. 同轴电缆　　B. 三类非屏蔽双绞线
C. 五类非屏蔽双绞线　　D. 光纤电缆

4.7.2 参考答案

1. D
2. C
3. C
4. (1) A　(2) C　(3) B　(4) B
5. A
6. D
7. (1) A　(2) B　(3) C　(4) A
8. C

第 5 章　无线通信网

大纲要求：

- 移动通信：蜂窝系统的原理，第二代移动通信技术 GSM 和 CDMA，第三代移动通信技术 CDMA2000、WCDMA 和 TD-SCDMA。
- 无线局域网：无线接入点(AP)和 Ad Hoc 网络、扩频通信技术 DSSS 和 HFSS、CSMA/CA 协议、802.11a/802.11b/802.11g、认证技术 WEP 和 802.11i。
- 无线个域网：蓝牙技术和 ZigBee。
- 无线城域网：无线城域网关键技术、WIMAX 技术、802.16e。

5.1　移 动 通 信

5.1.1　考点辅导

5.1.1.1　蜂窝通信系统

蜂窝通信系统也叫“小区制”系统，如图 5-1 所示，它将所有要覆盖的地区划分为若干个小区，每个小区的半径可视用户的分布密度在 1～10 km，形成了形状酷似“蜂窝”的结构，因而把这种移动通信方式称为蜂窝移动通信方式。在每个小区设立一个基站为本小区范围内的用户服务，并可通过小区分裂进一步提高系统容量。相邻小区不能使用相同的频率通信。当用户移动到一个小区的边缘时，电话信号的衰减程度提醒相邻的基站进行切换操作，正在通信的用户就自动切换到另一个小区的频段继续通话。

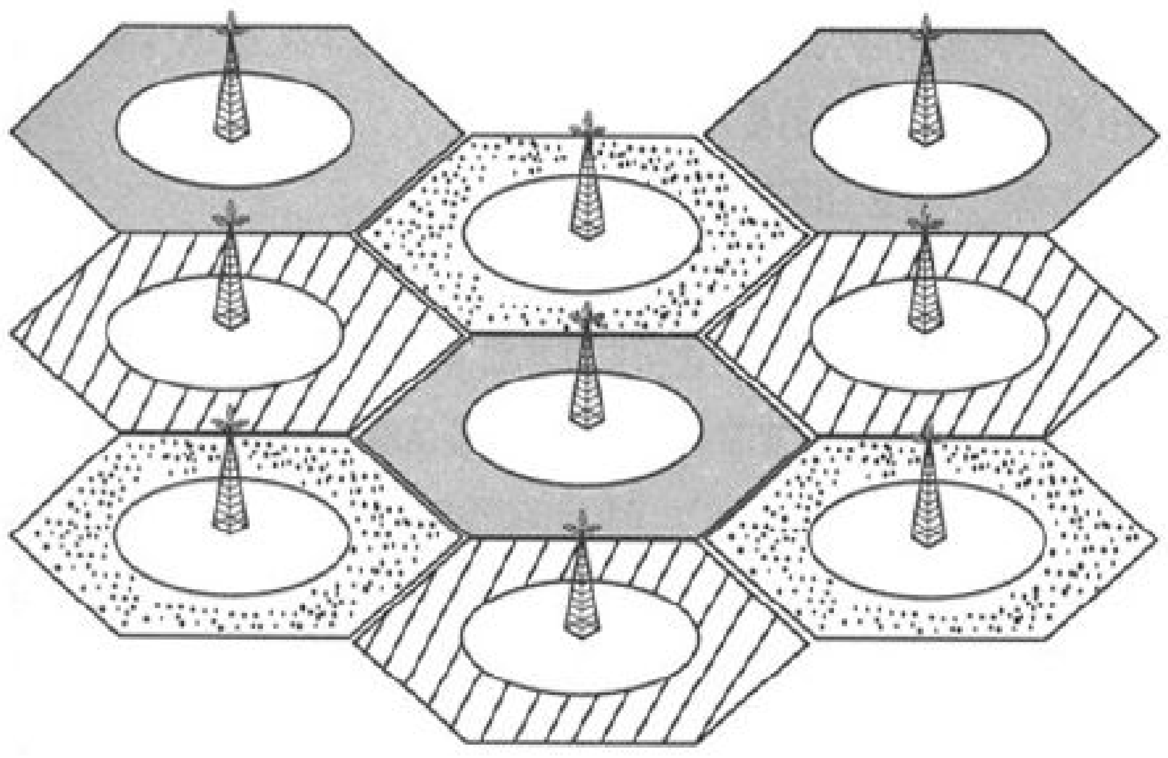


图 5-1　蜂窝通信系统

5.1.1.2　第二代移动通信系统

第二代移动通信系统是引入数字无线电技术组成的数字蜂窝移动通信系统，它提供更高的网络容量，改善了话音质量和保密性，并为用户提供无缝的国际漫游。在中国，第二代移动通信系统以 GSM 为主，CDMA 为辅。

1. 全球移动通信系统

目前，中国移动、中国联通各拥有一个全球移动通信系统(Global System for Mobile Communications，GSM)，为世界最大的移动通信网络。GSM 系统包括 GSM 900：900 MHz、GSM 1800、1800 MHz 及 GSM 1900：1900MHz 等几个频段。

2. 码分多址通信系统

美国高通公司的第二代数字蜂窝移动通信系统工作在 800MHz 频段，采用码分多址(CDMA)技术提供话音和数据业务。

CDMA 通信系统是基于码分技术(扩频技术)和多址技术的通信系统，系统为每个用户分配各自特定地址码，地址码之间具有相互准正交性，从而在时间、空间和频率上都可以重叠；将需传送的具有一定信号带宽的信息数据，用一个带宽远大于信号带宽的伪随机码进行调制，使原有的数据信号的带宽被扩展，接收端进行相反的过程，进行解扩，增强了抗干扰的能力。

3. 2.5G

2.5G 移动通信技术是从 2G 迈向 3G 的衔接性技术。由于 3G 是个相当浩大的工程，所牵扯的层面多且复杂，要从 2G 迈向 3G 不可能一下就衔接得上，因此出现了介于 2G 和 3G 之间的 2.5G。GPRS、HSCSD、WAP、EDGE、蓝牙(Bluetooth)、EPOC 等技术都是 2.5G 技术。

5.1.1.3 第三代移动通信系统

3G 是第三代移动通信技术，是指支持高速数据传输的蜂窝移动通信技术。3G 服务能够同时传送声音及数据信息，下行速度峰值理论可达 3.6Mb/s(一说 2.8Mb/s)，上行速度峰值可达 384kb/s。

中国国内支持国际电联确定 3 个无线接口标准，分别是中国电信的 CDMA 2000、中国联通的 WCDMA、中国移动的 TD-SCDMA。GSM 设备采用的是时分多址技术，而 CDMA 使用码分扩频技术，先进功率和话音激活至少可提供大于 3 倍的 GSM 网络容量，业界将 CDMA 技术作为 3G 的主流技术，国际电联确定 3 个无线接口标准，分别是美国 CDMA 2000、欧洲 WCDMA、中国 TD-SCDMA。原中国联通的 CDMA 卖给中国电信，中国电信已经将 CDMA 升级到 3G 网络，3G 主要特征是可提供移动宽带多媒体业务。

在 3G 网络广泛部署的同时，第四代(4G)移动通信系统也在加紧研发。高速分组接入(High Speed Packet Access，HSPA)是 WCDMA 第一个向 4G 进化的技术，继 HSPA 之后的高速上行分组接入(High Speed Uplink Packet Access，HSPA)是一种被称为 3.75G 的技术，在 5MHz 的载波上数据速率可达 10～15Mbps，如采用 MIMO 技术，还可以达到 28Mbps。

5.1.2 典型例题分析

例 5-1 关于移动 Ad Hoc 网络 MANET，__(63)__ 不是 MANET 的特点。(2015 年上半年真题 63)

A. 网络拓扑结构是动态变化的

B. 电源能量限制了无线终端必须以最节能的方式工作

C. 可以直接应用传统的路由协议支持最佳路由选择

D. 每个节点既是主机，又是路由器

解析：移动 Ad Hoc 网络(MANET)是一种与传统的有基站无线网络相对的无中心结构通信网，也被称为自组网。但无线网络的动态结构特点，以及无线终端的电源能量有限，使传统的路由协议不能直接应用于 MANET。目前已经提出了多种 MANET 路由协议，如目标排序的距离矢量协议(DSDV)、按需分配的距离矢量协议(AODV)等。

答案：C

5.1.3　同步练习

中国自主研发的 3G 通信标准是____。

A. CDMA2000　　B. TD-CSDMA　　C. WCDMA　　D. WiMAX

5.1.4　同步练习参考答案

B

5.2　无线局域网

5.2.1　考点辅导

5.2.1.1　无线局域网的基本概念

1. 无线局域网协议体系

(1) IEEE 802.11 协议标准体系：面向数据通信的计算机局域网发展而来的，采用的是无连接协议。

(2) HIPERLAN 协议标准体系：欧洲邮电委员会(CEPT)制定的，致力于面向语音的蜂窝电话，采用的是基于连接的协议。

2. 802.11 标准

IEEE 802.11 委员会相继制定了多种物理层标准。1997 年颁布的 IEEE 802.11 标准运行在 2.4GHz 的 ISM 段频，采用扩频通信技术，支持 1Mb/s 和 2Mb/s 的数据速率。随后又出现了两个新的标准：1998 年推出 IEEE 802.11b 标准，也是运行在 ISM 频段，采用 CCK 技术，支持 11Mb/s 的数据速率；1999 年推出 IEEE 802.11a 标准，运行在 U-NII 频段，采用 OFDM 调制技术，支持最高达 54Mb/s 的数据速率。目前的 WLAN 标准主要有 4 种，如表 5-1 所示。

表 5-1　IEEE 802.11 标准

名　称	发布时间	工作频段	调制技术	数据速率
802.11	1997 年	2.4GHz ISM 频段	DBPSK	1Mb/s
			DQPSK	2Mb/s
802.11b	1998 年	2.4GHz ISM 频段	CCK	5.5Mb/s、11Mb/s
802.11a	1999 年	5GHz U-NII 频段	OFDM	54Mb/s
802.11g	2003 年	2.4GHz ISM 频段	OFDM	54Mb/s

3. WLAN 的拓扑结构

IEEE 802.11 标准定义了两种无线网络的拓扑结构，一种是基础设施网络(Infrastructure Networking)，另一种是特殊网络(Ad Hoc Networking)。

- 在基础设施网络中，无线终端通过接入点访问骨干网设备，或者相互访问。
- Ad Hoc 网络是一种点对点连接，不需要有线网络和接入点的支持，以无线网卡连接的终端设备之间可以直接通信。这种拓扑结构适合在移动情况下快速部署网络，主要用在军事领域，也可以用在商业领域进行语音和数据传输。

5.2.1.2　WLAN 的通信技术

现在无线网主要使用 3 种通信技术：红外线、扩展频谱和窄带微波技术。这 3 种技术的主要特点如表 5-2 所示。

表 5-2　WLAN 通信技术的比较

类　别	红外线		扩展频谱		窄带微波
特　性	散射红外线	定向红外光束	频率跳动	直接序列	无线电
数据速率(Mbps)	1～4	10	1～3	2～20	5～10
移动特性	固定/移动	与 LOS 固定	移动	固定/移动	
范围(ft)	50～200	80	100～300	100～800	40～130
可监测性	可忽略		几乎无		有一些
波长/频率	λ：850～950nm		ISM 频带：902～928MHz 2.4～2.4835GHz 5.725～5.875GHz		18.825～19.025GHz 或 ISM 频带
调制技术	OOK		GFSK	QPSK	FSK/QPSK
辐射能量	NA		<1W		25mW
访问方法	CSMA	令牌环，CSMA	CSMA		预约 ALOHA，CSMA
需许可证否	否		否		除 ISM 外都要

5.2.1.3　IEEE 802.11 WLAN 的体系结构

IEEE 802.11 WLAN 的协议体系结构如图 5-2 所示。其中 LLC 子层与以太网一样都是 IEEE 802.2。

数据链路层	LLC		站管理
	MAC	MAC 管理	
物理层	PLCP	PHY 管理	
	PMD		

图 5-2　WLAN 体系结构

MAC 层分为 MAC 子层和 MAC 管理子层。MAC 子层负责访问和分组拆装，MAC 管理子层负责 ESS 漫游、电源管理和登记过程中的关联管理。物理层分为物理层汇聚协议(Physical Layer Convergence Protocol，PLCP)、物理介质相关(Physical Medium Dependent，PMD)子层和 PHY 管理子层。PLCP 子层主要进行载波监听和物理层分组的建立，PMD 子层用于传输信号的调制和编码，而 PHY 管理子层负责选择物理信道和调谐。

1. 物理层

IEEE 802.11 定义了 3 种 PLCP 帧格式来对应 3 种不同的 PMD 子层通信技术。

1)　FHSS

对应于 FHSS 通信的 PLCP 帧格式如图 5-3 所示。

SYNC(80)	SFD(16)	PLW(12)	PSF(4)	CRC(16)	MPDU(≤4096 字节)

图 5-3　用于 FHSS 方式的 PLCP 帧

SYNC 是 0 和 1 的序列，共 80 比特作为同步信号。SFD 的比特模式为 0000110010111101，用作帧的起始符。PLW 代表帧的长度，共 12 位，所以帧最大长度可以达到 4096 字节。PSF 是分组信令字段，用来标识不同的数据速率。起始数据速率为 1Mb/s，以 0.5 的步长递增。PSF=0000 时，代表数据速率为 1Mb/s；PSF 为其他数值时，则在起始速率的基础上增加一定倍数的步长，例如 PSF=0010，则 1Mb/s+0.5Mb/s×2=2Mb/s。16 位的 CRC 是为了保护 PLCP 头部所加的，它能纠正 2 比特错。MPDU 代表 MAC 协议数据单元。

2)　DSSS

图 5-4 所示为采用 DSSS 通信时的帧格式。

与前一种不同的字段解释如下：SFD 字段的比特模式为 1111001110100000。Signal 字段表示数据速率，步长为 100kb/s，比 FHSS 精确 5 倍。Service 字段保留未用。Length 字段指 MPDU 的长度。

SYNC(128)	SFD(16)	Signal(8)	Service(8)	Length(16)	FCS(8)	MPDU

图 5-4　用于 DSSS 方式的 PLCP 帧

3)　DFIR

图 5-5 所示为采用漫反射红外线时的 PLCP 帧格式。

SYNC(57～73)	SFD(4)	Data rate(3)	DCLA(32)	Length(16)	FCS(16)	MPDU

图 5-5　用于 DFIR 方式的 PLCP 帧

DFIR 的 SYNC 比 FHSS 和 DSSS 的都短，因为采用光敏二极管检测信号不需要复杂的

同步过程。Data rate 字段=000，表示 1Mb/s；Data rate 字段=001，表示 2Mb/s。DCLA 是直流电平调节字段，通过发送 32 个时隙的脉冲序列来确定接收信号的电平。MPDU 的长度不超过 2500 字节。

2. 802.11 MAC 子层

802.11 标准为 MAC 子层定义了 3 种访问控制机制：一是通过 CSMA/CA 方式进行分布式协调功能(DCF)，用于支持争用服务；二是通过点协调功能(PCF)来支持无争用服务；三是通过 RST/CST 来支持信道预约。图 5-6 所示是 DCF 和 PCF 之间的关系。

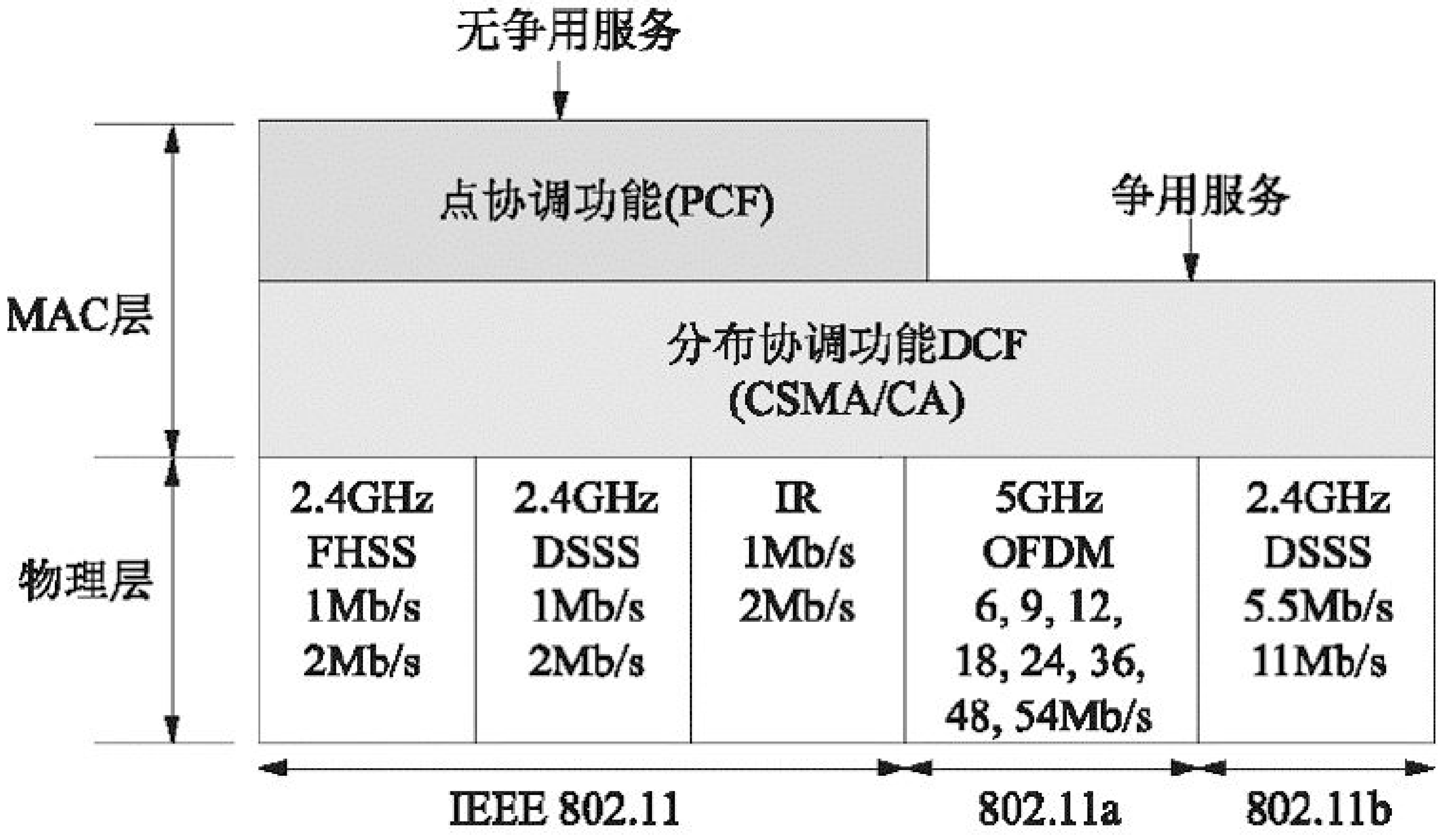


图 5-6　802.11 的 MAC 层

1)　CSMA/CA 协议

CSMA/CA 协议的工作原理如图 5-7 所示。

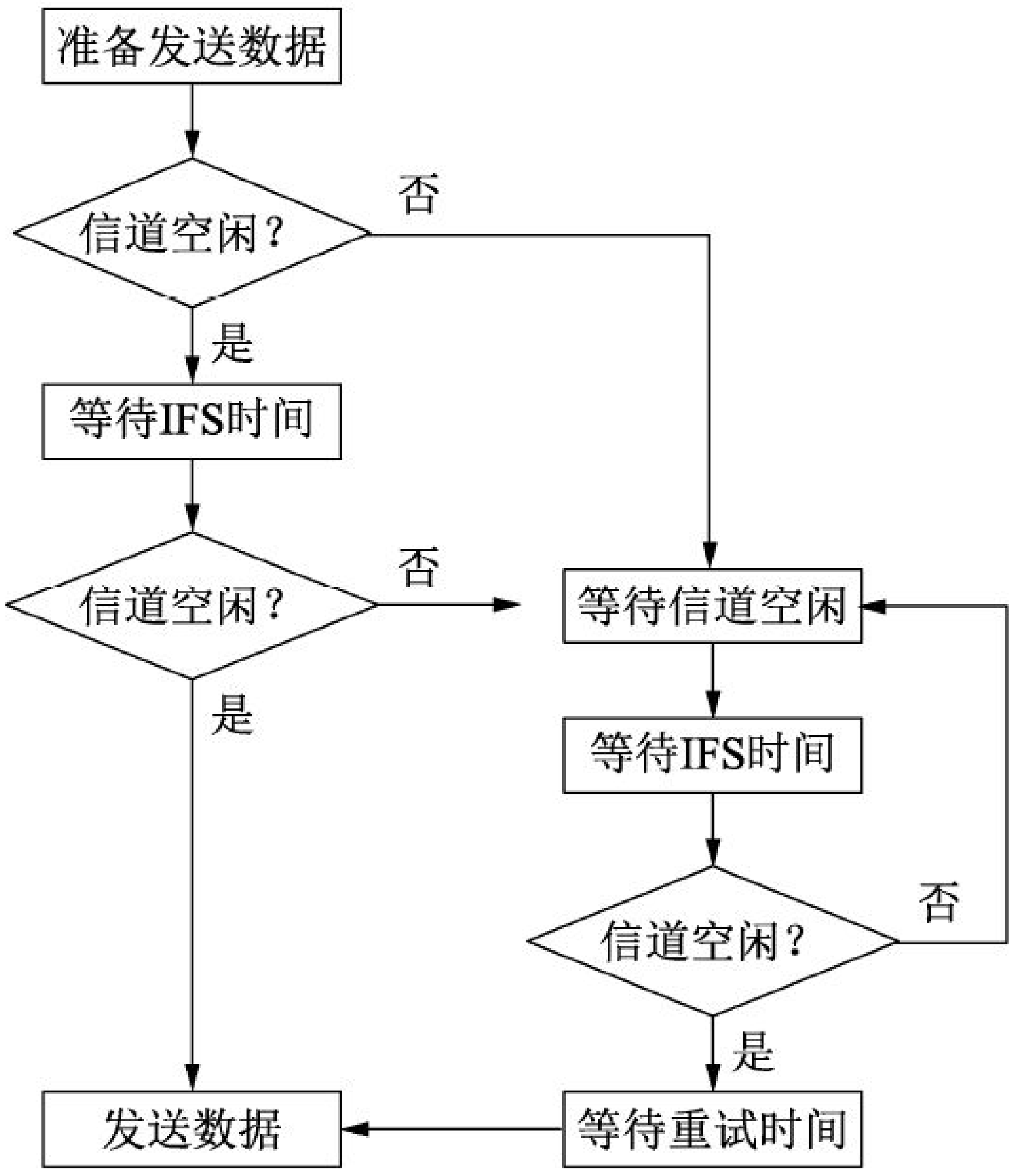


图 5-7　CSMA/CA 协议的工作原理

为了尽量避免碰撞，所有的站在完成发送后，必须再等待一段很短的时间(继续监听)才能发送下一帧。这段时间的通称是帧间间隔(IFS)。有 3 种帧间间隔。

- SIFS：短(Short)帧间间隔，长度为 28 μs，是最短的帧间间隔，用来分隔开属于一次对话的各帧。
- PIFS：点协调功能帧间间隔(比 SIFS 长)，是为了在开始使用 PCF 方式时(在 PCF 方式下使用，没有争用)优先获得接入到媒体中。PIFS 的长度是 SIFS 加一个时隙(slot)长度(其长度为 50μs)，即 78μs。
- DIFS：分布协调功能帧间间隔(最长的 IFS)，在 DCF 方式中用来发送数据帧和管理帧。DIFS 的长度比 PIFS 再增加一个时隙长度，因此 DIFS 的长度为 128μs。

2)　分布式协调功能(DCF)

802.11 MAC 层定义的分布式协调功能(Distributed Coordination Fuction，DCF)利用了 CSMA/CA 协议，在此基础上又定义了点协调功能(Point Coordination Fuction，PCF)。DCF 是数据传输的基本方式，作用于信道竞争期。PCF 工作于非竞争期。两者总是交替出现，先由 DCF 竞争介质使用权，然后进入非竞争期，由 PCF 控制数据传输。

3)　点协调功能(PCF)

PCF 是在 DCF 之上实现的一个可选功能，在 Ad-hoc 网络中没有 PCF。它由 AP 集中轮询所有移动站，将发送数据权轮流交给各个站，从而可避免碰撞的产生，为它们提供无争用服务。这种机制适用于对时间敏感的业务，如分组话音等。轮询过程中使用 PIFS 作为帧间隔时间。由于 PIFS 比 DIFS 小，因此点协调能够优先 CSMA/CA 获得信道，并把所有的异步帧都推后传送。

3. MAC 管理子层

WLAN 是开放系统，各站点共享传输介质，而且通信站具有移动性，因此，必须解决信息的同步问题、漫游问题、保密问题和节能问题。

1)　同步问题

信标是一种管理帧，由 AP 定期发送，用于进行时间同步。同步方式有主动扫描和被动扫描两种。

所谓主动扫描，就是终端在预定的各个频道上连续扫描，发射探试请求帧，并等待各个 AP 回答的响应帧；收到各 AP 的响应帧后，工作站将对各个帧中的相关部分进行比较以确定最佳 AP。

终端获得同步的另一种方法是被动扫描。如果终端已在 BSS 区域，那么它可以收到各个 AP 周期性发射的信标帧，因为帧中含有同步信息，所以工作站对各帧进行比较后，可确定最佳 AP。

2)　移动方式

IEEE 802.11 定义了 3 种移动方式：无转移方式、BSS 转移和 ESS 转移。

- 无转移方式是指终端是固定的，或者仅在 BSA 内部移动。
- BSS 转移是指终端在同一 ESS 内部的多个 BSS 之间移动。
- ESS 转移是指从一个 ESS 移动到另一个 ESS。

3)　安全管理

为了达到与有线网络同等的安全性能，IEEE 802.11 采取了认证和加密措施。

IEEE 802.11 提供的加密方式采用有线等价协议(Wired Equivalency Protocol，WEP)。WEP 是一种对称性的加密技术，即加密和解密都使用同样的算法和密钥，其加密算法是 RC4 流加密协议，密钥长度最初为 40 位(5 个字符)，后来增加到 128 位(16 个字符)。使用静态 WEP 加密，可以设置 4 个 WEP Key；使用动态 WEP 加密时，WEP Key 会随时间变化而变化。

2004 年 6 月公布的 IEEE 802.11i 标准是对 WEP 协议的改进。802.11i 定义了新的密钥交换协议(Temporal Key Integrity Protocol，TKIP)和高级加密标准(Advanced Encryption Standard，AES)。TKIP 提供了报文完整性检查，每个数据包使用不同的混合密钥(per-packet key mixing)，每次建立连接时生成一个新的基本密钥(re-keying)，这些手段的使用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力，从而消除了 WEP 协议的安全隐患。

4) 电源管理

IEEE 802.11 允许空闲站处于睡眠态，在同步时钟的控制下周期性地唤醒处于睡眠态的空闲站，由 AP 发送的信标帧中的 TIM(业务指示表)指示是否有数据暂存于 AP，若有，则向 AP 发探询帧，从 AP 接收数据，然后进入睡眠态；若无，则立即进入睡眠态。

5.2.1.4 移动 Ad Hoc 网络

与传统的有线网络相比，MANET 具有以下特点。

- 网络拓扑结构是动态变化的。
- 无线信道提供的带宽较小，而信号衰落和噪声干扰的影响却很大。
- 无线终端携带的电源能量有限。
- 由于无线链路的开放性，容易招致网络窃听、欺骗、拒绝服务等恶意攻击的威胁。

无线移动自组织网络中还有一种特殊的现象，就是隐蔽终端和暴露终端问题。

1. MANET 中的路由协议

根据路由策略，可分为表驱动路由协议和源路由协议；根据网络结构，可分为扁平的路由协议、分层的路由协议和基于地理信息的路由协议。表驱动路由协议和源路由协议都是扁平的路由协议。

根据设计原理，扁平的路由协议还可进一步划分为先验式(表驱动)路由和反应式(按需分配)路由，前者大部分是基于链路状态算法的，后者主要是基于距离矢量算法的。

先验式(Proactive)路由是表驱动型协议，通过周期性地交换路由信息，每个节点可以保存完整的网络拓扑结构图，因而可以主动确定网络布局。按需分配的路由协议提供了可伸缩的路由解决方案。其主要思想是，移动节点只是在需要通信时才发送路由请求分组，以此来减少路由开销。

当网络规模扩大时，扁平路由协议产生的路由开销迅速增大，先验式路由会由于周期性交换链路状态信息而消耗太多的带宽，即使是反应式路由，也会由于越来越长的数据通路需要频繁维护而产生过多的控制开销。在这种情况下，采用分层的方案是一种较好的选择。

地理信息路由协议要求所有的节点都必须及时地访问地理坐标系统。例如，地理寻址路由协议。

2. DSDV 协议

DSDV(Destination Sequenced Distance Vector，目标排序的距离矢量)协议是由 Perkins 和 P. B hagwat 于 1994 年提出的一种基于 Bellman-Ford 算法的表驱动路由方案。DSDV 协议是一种扁平式路由协议。DSDV 协议的路由表项中包含目标地址、下一跳地址、跳步数、序列号、安装时间、稳定数据等字段。

DSDV 的节点周期性地广播路由公告，但是在出现新链路或者老链路断开时立即触发链路公告。

当一个节点接收到邻居节点发送的路由公告时，根据下列规则进行路由更新：对应于某个标的路由表项，如果收到的序列号比路由表中已有的序列号更大，则更新现有的路由表项；如果收到的序列号和现有的序列号相同，但度量值更小，也要更新现有的路由表项；否则放弃收到的路由更新公告，维持现有的路由表项不变。

通过序列号机制可以排除路由环路现象。但 DSDV 要解决路由波动问题。为了解决这个问题，DSDV 采用平均定制时间(Average Setting Time，AST)来决定发布路由公告的时间间隔，AST 表示对应目标节点更新路由的平均时间间隔，而最近定制时间(Last Setting Time，LST)则是最近一次更新路由的时间间隔。第 n 次的平均定制时间是最近定制时间与前 $n-1$ 次的平均定制时间的加权平均值，即

$$\mathrm{AST}_n=\frac{2\mathrm{LST}+\mathrm{AST}_{n-1}}{3}$$

为了减少路由波动，节点可以等待两倍的 AST_n 时间再发送路由公告。

3. AODV 协议

按需分配的距离矢量(Ad hoc On-Demand Distance Vector，AODV)协议也是一种扁平式路由协议，但是采用了反应式路由策略。

AODV 协议采用了类似于 DSDV 协议的序列号机制，用于排除一般距离矢量协议可能引起的路由环路问题。AODV 协议的路由表项由下列字段组成：目标 IP 地址、目标子网掩码、目标序列号、下一跳 IP 地址、路由表项的生命周期、度量值/跳步数、网络接口、其他的状态和路由标志。

AODV 协议是一种按需分配的路由协议，当一个节点需要发送到达某个目标节点的路由时就广播路由请求(Route Request，RREQ)报文。

当一个节点接收到 RREQ 报文时，如果它就是请求的目标，或者知道到达目标的路由并且其中的目标序列号大于 RREQ 中的目标序列号，则要响应这个请求，向发送 RREQ 的节点返回(单播)一个路由应答(Route Reply，RREP)报文。如果收到 RREQ 报文的节点不知道该目标的路由，则它要重新广播 RREQ 报文，并且记录发送 RREQ 报文的节点 IP 地址及其广播序列号(RREQ ID)。如果收到的 RREQ 报文已经被处理过了，则丢弃该报文，不再进行转发。

AODV 协议也适用于组播网络。

5.2.1.5　IEEE 802.11 的新进展

无线局域网面临着两个主要问题，一是增强安全性，二是提高数据速率。

1. WLAN 的安全

1) SSID 访问控制

可以对各个无线接入点(AP)设置不同的 SSID(Service Set Identifier)，当然，也可以禁用 SSID 广播。

2) 物理地址过滤

在无线路由器中维护一组允许访问的 MAC 地址列表，用于实现物理地址过滤功能。

3) 有线等效保密

有线等效保密(Wired Equivalent Privacy，WEP)使用 RC4 协议进行加密，并使用 CRC-32 校验保证数据的正确性。最初的 WEP 标准使用 24 位的初始向量，加上 40 位的字符串，构成 64 位的 WEP 密钥。后来美国政府放宽了出口密钥长度的限制，允许使用 104 位的字符串，加上 24 位的初始向量，构成 128 位的 WEP 密钥。

4) WPA

Wi-Fi 联盟的厂商们以 802.11i 草案的一个子集为蓝图制定了称为 WPA(Wi-Fi Protected Access)的安全认证方案。在 WPA 的设计中包含了认证、加密和数据完整性校验 3 个组成部分。

首先是 WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度，以及 128 位的密钥和 48 位的初始向量(IV)用于 RC4 加密。WPA 还采用了可以动态改变密钥的临时密钥完整性协议(Temporary Key Integrity Protocol，TKIP)，通过更频繁地变换密钥来降低安全风险。

5) IEEE 802.11i

IEEE 802.11i 标准包含以下 3 个方面的安全部件。

- 临时密钥完整性协议(TKIP)是一个短期的解决方案，仍然使用 RC4 加密方法，但是弥补了 WEP 的安全缺陷。
- 重新制定了新的加密协议，称为 CBC-MAC 协议的计时器模式(Counter Mode with CBC-MAC Protocol，CCMP)。这是基于高级加密标准(Advanced Encryption Standard，AES)的加密方法。
- 采用 802.1x 进行身份认证。如果认证通过，则 AP 为无线工作站打开一个逻辑端口。

可扩展的认证协议(Extensible Authentication Protocol，EAP)是一种专门用于认证的传输协议。常用的认证机制有 EAP-MD5、Lightweight EAP (LEAP)、EAP-TLS。

802.11i 还提供了一种任选的加密方案 WRAP(Wireless Robust Authentication Protocol)，实现了一种动态密钥交换和管理体制。对于小型办公室和家庭应用，可以使用预共享密钥(Pre-Shared Key，PSK)的方案，这样就可以省去 802.1x 认证和密钥交换过程了。

2. WLAN 的传输速率

2009 年 9 月 11 日 IEEE 802.lln 标准正式发布。802.11n 结合了 MIMO 与 OFDM 技术，可以将 WLAN 的传输速率由目前 802.11a/802.11g 的 54Mbps 提高到 300Mbps，甚至 600Mbps。

正交频分复用(Orthogonal Frequency Division Multiplexing，OFDM)是一种多载波调制技

术。其主要思想是将信道划分成若干个正交子信道，将高速数据信号转换成并行的低速子数据流，并将各个子数据流交织编码，调制到正交的子信道上进行传输，在接收端采用相关技术可以将正交信号再分开。OFDM 具有较高的频谱利用率。

MIMO(Multiple Input Multiple Output，多入多出)是通过多径无线信道实现的，传输的信息流经过空时编码成 N 个子信息流，由 N 个天线发射出去，经空间信道传输后由 M 个接收天线接收。多天线接收机利用先进的空时编码处理功能对数据流进行分离和解码，从而实现最佳的处理结果。

5.2.2　典型例题分析

例 5-2　无线局域网通常采用的加密方式是 WPA2，其安全加密算法是<u>　(44)　</u>。(2017 年下半年真题 44)

A. AES 和 TKIP　　B. DES 和 TKIP　　C. AES 和 RSA　　D. DES 和 RSA

解析：WPA2 避免了 WEP 的相关问题，它使用 AES 加密数据，并定义了一个具有更高安全性的加密标准 CCMP，密码使用 TKIP 方式。

答案：A

例 5-3　在以太网中出于对<u>　(64)　</u>的考虑，需设置数据帧的最小帧。(2017 年上半年真题 64)

A. 重传策略　　B. 故障检测　　C. 冲突检测　　D. 提高速率

解析：为了确保发送数据站点在传输时能检测到可能发生的冲突，数据帧的传输时延要不小于两倍的传播时延。

答案：C

例 5-4　802.11g 的最高数据传输速率为<u>　(66)　</u>Mbps。(2017 年上半年真题 66)

A. 11　　B. 28　　C. 54　　D. 108

解析：802.11g 运行频段为 2.4GHz 的 ISM 频段，使用的主要技术是 ODDM 调制技术，其数据速率为 54Mbps。

答案：C

例 5-5　IEEE 802.11 标准采用的工作频段是<u>　(65)　</u>。(2016 年下半年真题 65)

A. 900MHz 和 800MHz　　B. 900MHz 和 2.4GHz

C. 5GHz 和 800MHz　　D. 2.4GHz 和 5GHz

解析：IEEE 802.11 标准采用的工作频段是 2.4GHz 和 5GHz。

答案：D

例 5-6　IEEE 802.11 MAC 子层定义的竞争性访问控制协议是<u>　(66)　</u>。(2016 年下半年真题 66)

A. CSMA/CA　　B. CSMA/CB　　C. CSMA/CD　　D. CSMA/CG

解析：CSMA/CD 虽然已经成功应用于适用有线连接的局域网，但在无线局域网的环境下，不能简单地搬运，特别是冲突检测部分，IEEE 802.11 MAC 子层定义的竞争性访问控制协议是 CSMA/CA。

答案：　A

例 5-7 无线局域网的新标准 IEEE 802.11n 提供的最高数据速率可达到__(67)__Mb/s。(2016 年下半年真题 67)

A. 54　　B. 100　　C. 200　　D. 300

解析：802.11n 可工作在 2.4GHz 和 5GHz 两个频段，速率可达到 300Mbps，使用 MIMO 技术可以达到 600Mbps。

答案：D

例 5-8 IEEE 802.11 MAC 子层定义的竞争性访问控制协议是__(65)__。之所以不采用与 IEEE 802.3 相同协议的原因是__(66)__。(2016 年上半年真题 65、66)

(65) A. CSMA/CA　　B. CSMA/CB　　C. CSMA/CD　　D. CSMA/CG

(66) A. IEEE 802. 11 协议的效率更高

B. 为了解决隐蔽终端问题

C. IEEE 802. 3 协议的开销更大

D. 为了引进多种非竞争业务

解析：CSMA/CD 协议已经成功运用于用有线连接的局域网，但在无线局域网的环境下，不能简单搬用 CSMA/CD 协议，特别是冲突检测部分。主要原因有两个:

① 在无线局域网中，接收信号的强度往往会远小于发送信号的强度，因此如果要实现冲突检测的话，在硬件上的花费就会比较大。

② 在无线局域网中，并非所有的站点都能监听到对方，而“所有站点都能监听到对方”正是 CSMA/CD 协议的基础。

CSMA/CD: 带有冲突检测的载波监听多路访问，可以检测冲突，但无法“避免”。

CSMA/CA: 带有冲突避免的载波监听多路访问，发送包的同时不能检测到信道上有无冲突，只能尽量“避免”。

答案：(65) A　(66) B

例 5-9 以下关于 CSMA/CD 协议的叙述中，正确的是__(62)__。(2015 年下半年真题 62)

A. 每个节点按照逻辑顺序占用一个时间片轮流发送

B. 每个节点检查介质是否空闲，如果空闲则立即发送

C. 每个节点想发就发，如果没有冲突则继续发送

D. 得到令牌的节点发送，没有得到令牌的节点等待

解析：每个以太网节点利用总线发送数据时，首先需要侦听总线是否空闲。以太网的物理层规定发送的数据采用曼彻斯特编码方式。如果总线上已经没有数据在传输，总线的电平将不会发生跳变，可以判断此时为“总线空闲”。如果一个节点已准备好发送的数据帧，并且总线此时处于空闲状态，则这个节点就可以“启动发送”。

答案：B

例 5-10 为了弥补 WEP 协议的安全缺陷，WPA 安全认证方案增加的机制是__(50)__。(2015 年上半年真题 50)

A. 共享密钥认证　　B. 临时密钥完整性协议

C. 较短的初始化向量　　D. 采用更强的加密算法

解析：在 WPA 的设计中包含了认证、加密和数据完整性校验 3 个组成部分。首先是

WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度；WPA 还采用了可以动态改变密钥的临时密钥完整性协议(TKIP)；最后，WPA 强化了数据完整性保护。

答案：B

5.2.3　同步练习

1. 在无线局域网中，AP(无线接入点)工作在 OSI 模型的________。

A. 物理层　　B. 数据链路层　　C. 网络层　　D. 应用层

2. 以太网采用的 CSMA/CD 协议，当冲突发生时要通过二进制指数后退算法计算后退时延，关于这个算法，以下论述中错误的是________。

A. 冲突次数越多，后退的时间越短　　B. 平均后退次数的多少与负载大小有关

C. 后退时延的平均值与负载大小有关　　D. 重发次数达到一定极限后放弃发送

3. 以下通信技术中，未在 IEEE 802.11 无线局域网中使用的是________。

A. FHSS　　B. DSSS　　C. CDMA　　D. IR

4. IEEE 802.11 规定了多种 WLAN 的通信标准，其中________与其他标准采用频段不同，因而不能兼容。

A. IEEE 802.11a　　B. IEEE 802.11b　　C. IEEE 802.11g　　D. IEEE 802.11n

5. IEEE 802.11 定义的 Ad Hoc 网络是由无线移动节点组成的对等网，这种网络的特点是__(1)__。在这种网络中使用的 DSDV(Destination-Sequenced Distance Vector)路由协议是一种__(2)__。

(1) A. 每个节点既是主机，又是交换机

B. 每个节点既是主机，又是路由器

C. 每个节点都必须通过中心节点才能互相通信

D. 每个节点都发送 IP 广播包来与其他节点通信

(2) A. 洪泛式路由协议　　B. 随机式路由协议

C. 链路状态路由协议　　D. 距离矢量路由协议

5.2.4　同步练习参考答案

1. B　　2. A　　3. C　　4. A　　5. (1) B　(2) D

5.3　无线个域网

5.3.1　考点辅导

1998 年，IEEE 802.15 工作组成立，专门从事 WPAN 标准化工作。它的任务是开发一

套适用于短程无线通信的标准，通常我们称之为无线个人局域网(WPAN)。

目前，IEEE 802.15 WPAN 共拥有 4 个工作组。

(1) 蓝牙 WPAN 工作组(802.15.1)：蓝牙是无线个人局域网的先驱。在初始阶段，IEEE 并没有制定蓝牙相关的标准，所以经过一段快速发展时期后，蓝牙很快就有了产品兼容性的问题。现在，IEEE 决定制定行业标准来开发能够相互兼容的蓝牙芯片、网络和产品。

(2) 共存组(802.15.2)：为所有工作在 2.4GHz 频带上的无线应用建立一个标准。

(3) 高数据率 WPAN 工作组(802.15.3)：其 802.15.3 标准适用于高质量要求的多媒体应用领域。

(4) 802.15.4 工作组(802.15.4)：为了满足低功耗、低成本的无线网络要求，IEEE 标准委员会在 2000 年 12 月份正式批准并成立了 802.15.4 工作组，任务就是开发一个低数据率的 WPAN(LR-WPAN)标准。它具有复杂度低、成本极小、功耗很小的特点，能在低成本设备(固定、便携或可移动的)之间进行低数据率的传输。

5.3.1.1 蓝牙技术

蓝牙(Bluetooth)无线技术是一种短距离通信技术，旨在取代电缆来连接便携式和/或固定设备，并保证高度安全性。Bluetooth 技术的主要特点在于功能强大、耗电量低、成本低廉。Bluetooth 规格为广泛范围的设备定义了统一的结构，以便于彼此之间进行连接和通信。

Bluetooth 技术已获得了全球认可，世界各地的 Bluetooth 设备都可以与其邻近的 Bluetooth 设备连接。Bluetooth 电子设备可以通过短距离的即时网络(称为微微网)进行无线连接和通信。每个设备最多可以在微微网中同时与 7 个其他设备进行通信。每个设备还可以同时属于多个微微网。当 Bluetooth 设备进入然后离开无线电邻近区域时，微微网可在此期间自动动态建立。

Bluetooth 无线技术的基本优势在于它可以同时处理数据和语音传输。这使得用户可以享受各种创新解决方案，如免提耳机接听语音电话、打印和传真功能、同步 PDA、膝上型计算机和手机应用程序，等等。

1. 核心系统的体系结构

蓝牙核心系统的体系结构如图 5-8 所示。

最下面的 Radio 层相当于 OSI 的物理层，其中的 RF 模块采用 2.4GHz 的 ISM 频段实现跳频通信(FHSS)，信号速率为 1Mbps，数据速率为 1Mbps。物理信道被划分为时槽，数据被封装成分组，每个分组占用一个时槽。在一对收发设备之间可以用时分多路(TTD)方式实现全双工通信。

物理信道之上是各种链路和信道层及其有关的协议。以物理信道为基础，向上依次形成的信道层次为物理信道、物理链路、逻辑传输、逻辑链路和 L2CAP (Logical Link Control and Adaptation Protocol)信道。

一条物理链路可以支持多条逻辑链路，只有逻辑链路才可以进行单播同步通信、异步等时通信或者广播通信，不同的逻辑链路用于支持不同的应用需求。

基带层和物理层的控制协议叫作链路管理协议(Link Manager Protocol，LMP)，用于控制设备的运行，并提供底层设施(PHY 和 BB)的管理服务。

逻辑链路控制和自适应协议(L2CAP)是对应用和服务的抽象，其功能是对应用数据进行

分段和重装配，并实现逻辑链路的复用。

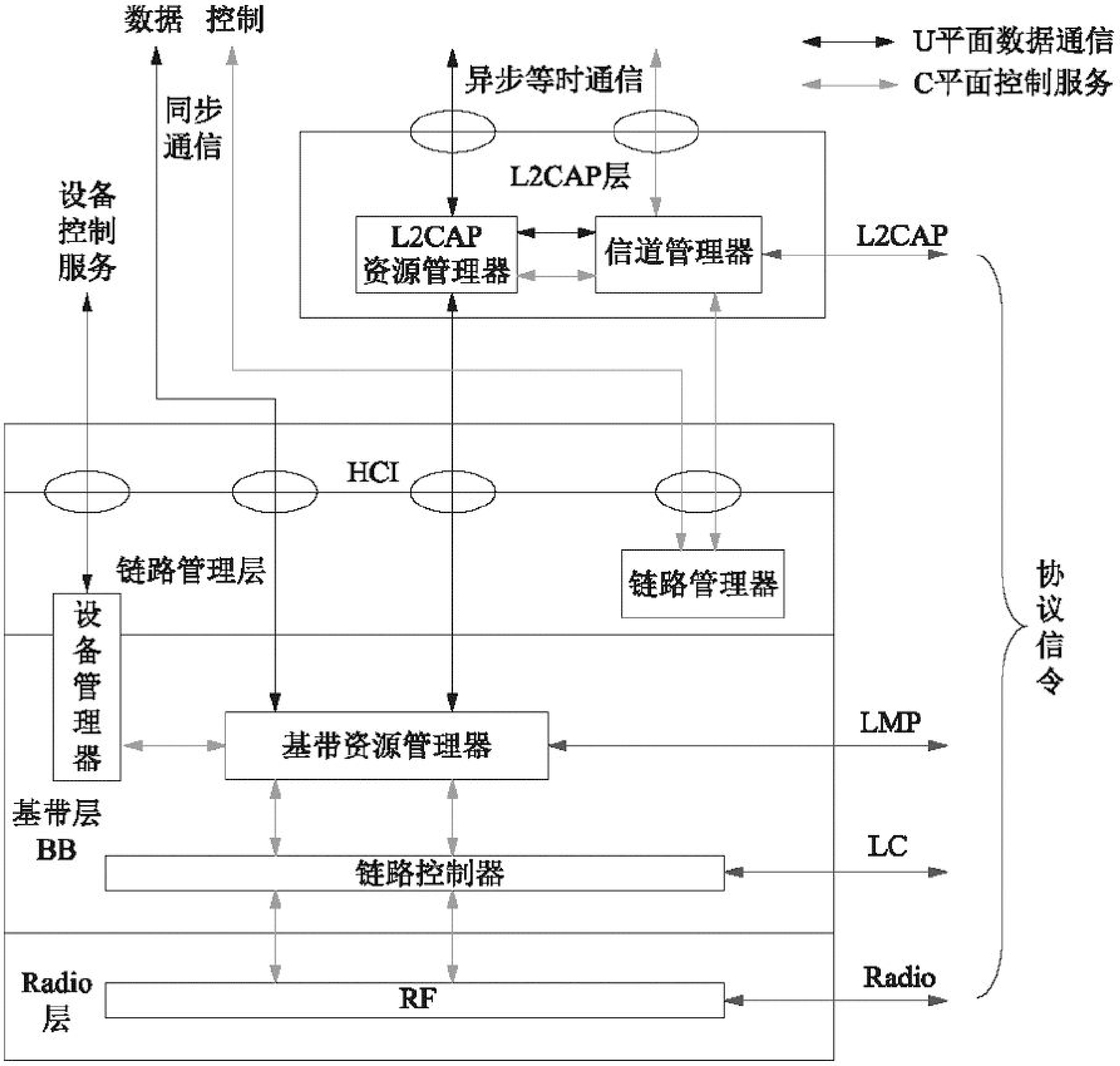


图 5-8　蓝牙核心系统体系结构

设备之间的互操作通过核心系统协议实现，主要的协议有 RF (Radio Frequency)协议、链路控制协议(Link Control Protocol，LCP)、链路管理协议(LMP)和 L2CAP。

蓝牙控制器与高层之间的接口叫作主机控制器接口(Host Controller Interface，HCI)。

2. 核心功能模块

(1) 信道管理器：负责生成、管理和释放用于传输应用数据流的 L2CAP 信道。

(2) L2CAP 资源管理器：把 L2CAP 数据单元分段，并按照一定的顺序提交给基带层，而且还要进行信道调度，以保证一定 QoS 的 L2CAP 信道不会被物理信道(由于资源耗尽)拒绝。

(3) 设备管理器：负责控制设备的一般行为。

(4) 链路管理器(LM)：负责生成、修改和释放逻辑链路及其相关的逻辑传输，并修改设备之间的物理链路参数。

(5) 基带资源管理器：负责对物理层的访问。它有两个主要功能，其一是调度功能，其二是与这些实体协商包含 QoS 承诺的访问合同。

(6) 链路控制器：负责根据数据负载和物理信道、逻辑传输和逻辑链路的参数对分组进行编码和译码。

(7) RF (Radio Frequency)：用于发送和接收物理信道上的数据分组。

3. 数据传输结构

L2CAP 服务对于异步的和等时的用户数据提供面向帧的传输。面向连接的 L2CAP 信道用于传输点对点单播数据。无连接的 L2CAP 信道用于广播数据。

L2CAP 信道的 QoS 设置定义了帧传送的限制条件；非帧的流式数据使用 SCO 逻辑传输。

核心系统支持通过 SCO (SCO-S)或扩展的 SCO (eSCO-S)直接传输等时的和固定速率的应用数据。应用从 BB 层选择最适当的逻辑链路类型来传输它的数据流。RF 信道通常是不可靠的，因此 BB 分组头使用了纠错编码，并且配合头校验和来发现残余差错。在 ACL 逻辑传输中实现了 ARQ 协议，通过自动请求重发来纠正错误。

5.3.1.2 ZigBee 技术

ZigBee 是基于 IEEE 802.15.4 开发的一组关于组网、安全和应用软件的技术标准。

1. IEEE 802.15.4 标准

802.15.4 定义的低速无线个人网(Low Rate-WPAN)包含两类设备，即全功能设备(FFD)和简单功能设备(RFD)。FFD 有 3 种工作模式，可以作为一般的设备、协调器或 PAN 协调器。FFD 可以与 RFD 或其他 FFD 通信，而 RFD 只能与 FFD 通信，RFD 之间不能互相通信。

LR-WPAN 的拓扑结构有星型网络和点对点网络两种。在星型拓扑中，只有在设备和 PAN 协调器之间才能通信，在设备之间不能互相通信。点对点网络与星型网络不同，这种网络中的所有设备之间都可以互相通信，只要处于信号覆盖范围之内。

802.15.4 的体系结构如图 5-9 所示，物理层(PHY)包含 RF 收发器和底层管理功能，通过物理层管理实体服务访问点(PLME-SAP)和物理数据服务访问点(PD-SAP)向上层提供服务。

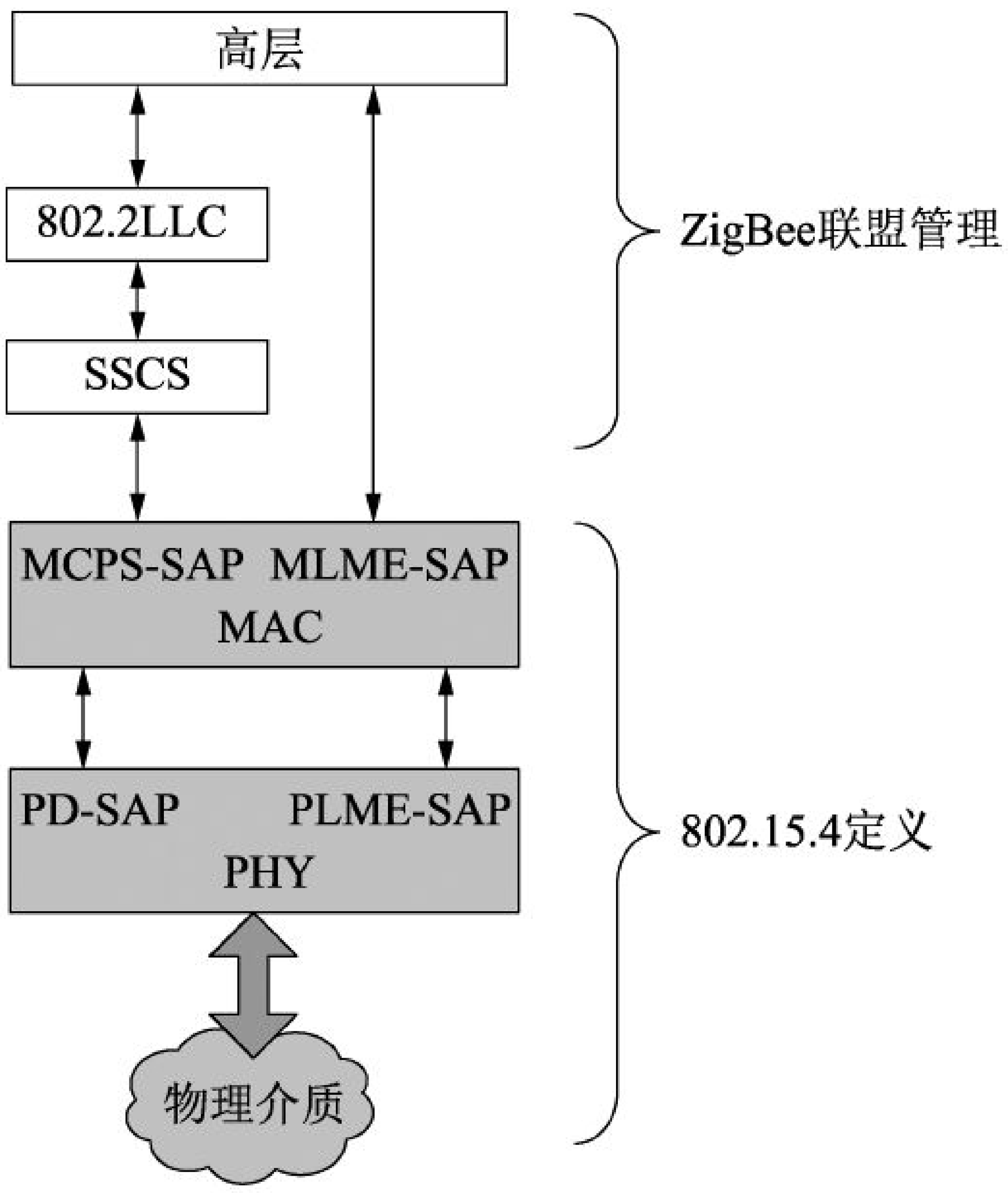


图 5-9 LR-WPAN 体系结构

802.15.4-2006 标准定义的 4 种物理层如下。

868～915MHz：直接序列扩频(DSSS)，二进制相移键控(B/SK)调制，数据速率为 20kb/s 和 40kb/s。

868～915MHz：直接序列扩频(DSSS)，偏置正交相移键控(O-QPSK)调制，数据速率为 100kb/s 和 250kb/s。

868～915MHz：并行序列扩频(PSSS)，二进制相移键控(B/SK)调制和幅度键控(ASK)调制，数据速率为 250kb/s。

2.450GHz：直接序列扩频(DSSS)，偏置正交相移键控(O-QPSK)调制，数据速率为 250kb/s。

MAC 子层提供两种信道访问方式，即基于竞争的访问和无竞争的访问。基于竞争的访问方式应用了 CSIVIA/CA 后退算法，而且划分为不分时槽的和分时槽的两个不同版本。不分时槽的 CSMA/CA 协议应用在未启用令牌的网络中，在启用令牌的网络中必须使用 CSMA/CA 协议的分时槽版本。

2. ZigBee 网络

ZigBee 联盟主要任务如下。

(1) 定义 ZigBee 的网络层、安全层和应用层标准。

(2) 提供互操作性和一致性测试规范。

(3) 促进 ZigBee 品牌的全球化市场保证。

(4) 管理 ZigBee 技术的演变。

ZigBee 技术规范(2005)描述了 ZigBee 网络的基础结构和可利用的服务。ZigBee 网络层(NWK)提供了建立多跳网络的路由功能。APL 层包含了应用支持子层(APS)和 ZigBee 设备对象(ZDO)，以及各种可能的应用。ZDO 的作用是提供全面的设备管理，APS 的功能是为 ZDO 和各种应用提供服务。

ZigBee 的安全机制分散在 MAC、NWK 和 APS 层，分别对 MAC 帧、NWK 帧和应用数据进行安全保护。ZigBee 的网络层和 MAC 层都使用高级加密标准(AES)，以及结合了加密和认证功能的 CCM*分组加密算法。

ZigBee 协调器管理网络的路由功能。ZigBee 采用的路由算法是按需分配的距离矢量(AODV)协议。当 NWK 数据实体要发送数据分组时，如果路由表中不存在有效的路由表项，则首先要进行路由发现，并对找到的各个路由计算通路费用。

5.3.2　典型例题分析

例 5-11　ZigBee 网络是 IEEE 802.15.4 定义的低速无线个人网，其中包含全功能和简单功能两类设备，以下关于这两类设备的描述中，错误的是__(65)__。(2014 年下半年真题 65)

A. 协调器是一种全功能设备，只能作为 PAN 的控制器使用

B. 被动式红外传感器是一种简单功能设备，接受协调器的控制

C. 协调器也可以运行某些应用，发起和接受其他设备的通信请求

D. 简单功能设备之间不能互相通信，只能与协调器通信

解析：ZigBee 网络中包含全功能(FFD)和简单功能(RFD)两类设备，在一个 ZigBee 网络中，至少存在一个 FFD 充当整个网络的协调器，即 PAN 协调器，ZigBee 中也称作 ZigBee 协调器。一个 ZigBee 网络只有一个 PAN 协调器。通常，PAN 协调器是一个特殊的 FFD，它具有较强大的功能，是整个网络的主要控制者，它负责建立新的网络、发送网络信标、管理网络中的节点以及存储网络信息等。FFD 和 RFD 都可以作为终端节点加入网络。

答案：A

5.4 无线城域网

5.4.1 考点辅导

无线城域网目前比较成熟的标准有两个，一个是 2004 年颁布的 802.16d，这个标准支持无线固定接入，也叫作固定 WiMAX；另一个是 2005 年颁布的 802.16e，它是在前一标准的基础上增加了对移动性的支持，所以也称为移动 WiMAX。

WiMAX 技术主要有两个应用领域，一个是作为蜂窝网络、Wi-Fi 热点和 Wi-Fi Mesh 的回程链路；另一个是作为最后 1km 的无线宽带接入链路。

移动 WiMAX (802.16e)向下兼容 802.16d，在移动性方面定位的目标速率与汽车速度相当，可以支持 120km/h 的移动速率。IEEE 802.16 的协议栈模型由物理层和 MAC 层组成，MAC 层又分成了 3 个子层，即面向服务的汇聚子层、公共部分子层和安全子层。

5.4.1.1 关键技术

802.16 系统采用两个工作频段，其中，10～66GHz 频段的工作波长较短，只能进行视距传输，在这个频段可以采用单载波调制方式。在 2～11GHz 频段可以进行非视距传输，但必须考虑多径衰减的影响，这时每个子载波的调制方式可以选用 B/SK、QPSK、16-QAM 或 64-QAM。

802.16 采用的多路复用方式 OFDM/OFDMA 被认为是下一代无线通信网的关键技术。正交频分多址(OFDMA)是利用 OFDM 的概念实现上行多址接入。OFDMA 的引入是为了支持移动性。为了进一步提高带宽利用率，802.16 还引入了多入多出技术(MIMO)。

802.16 系统以频分双工(FDD)或时分双工(TDD)方式工作。FDD 需要成对的频率，TDD 则不需要。

5.4.1.2 MAC 子层

802.16 MAC 层提供面向连接的服务。MAC 层定义了两种 CS 子层，即 ATM CS 和分组 CS，前者提供对 ATM 的业务支持，后者提供对 IEEE 802.3、IEEE 802.lq、IPv4 和 IPv6 等基于分组的业务的映射。

802.16 MAC 层定义了完整的 QoS 机制。为了更好地控制带宽分配，MAC 层定义了 4 种不同的业务。

(1) 非请求的带宽分配业务(UGS)：用于传输周期性的、包大小固定的实时数据，其典

型的应用是 VoIP 电话。

(2) 实时轮询业务(rtPS)：用于支持周期性的、包大小可变的实时业务，例如 MPEG 视频业务。

(3) 非实时轮询业务(nrtPS)：用于支持非实时可变速率业务，例如高带宽的 FTP 应用。

(4) 尽力而为业务(BE)：用于支持非实时性、无任何速率和时延要求的分组业务，典型业务是 Telnet 和 HTTP 服务。

5.4.1.3　向 4G 迈进

1. 802.16e

802.16d 的 OFDM 调制方式采用 256 个子载波，OFDMA 调制方式采用 2048 个子载波，信号带宽在 1.25～20MHz 可变。为了支持移动性，802.16e 对物理层进行了改进，使得 OFDMA 可支持 128、512、1024 和 2048 共 4 种不同的子载波数量，但子载波间隔不变，信号带宽与子载波数量成正比，这种技术被称为可扩展的 OFDMA (Scalable OFDMA)。采用这种技术，系统可以在移动环境中灵活地适应信道带宽的变化。在采用 20MHz 带宽、64-QAM 调制的情况下，传输速率可达到 74.81Mbps。

2. WiMAXII

ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速声音、数据和流式多媒体服务，支持的数据速率至少是 100Mbps，选定的通信技术是正交频分多址接入(OFDMA)技术。

最初候选的 4G 标准有 3 个，即 UMB(Ultra Mobile Broadband)、LTE(Long Term Evolution) 和 WiMAX II (IEEE 802.16m)。

(1) UMB 的最高下载速率可达到 288Mbps，最高上传速率可达到 75Mbps，支持的终端移动速率超过 300km/h。2008 年 11 月，高通公司宣布放弃 UMB 技术。

(2) LTE (Long Term Evolution)采用 OFDM/OFDMA 作为物理层的核心技术，支持 1.25～20MHz 宽带，峰值速率下行 1Gbps，上行 500Mbps。

(3) IEEE 802.16m 支持 5～20MHz 的可变带宽，特殊情况下可达 100MHz，其下行峰值速率在低速移动、热点覆盖条件下可以达到 1Gbps，在高速移动、广域覆盖条件下可以达到 100Mbps。

2013 年底，工信部正式向三大运营商发放了 4G 牌照，中国移动、中国电信和中国联通均获得 TD-LTE 牌照。

(1) 中国移动：1880～1900MHz、2320～2370MHz、2575～2635MHz。

(2) 中国联通：2300～2320MHz、2555～2575MHz。

(3) 中国电信：2370～2390MHz、2635～2655MHz。

5.4.2　典型例题分析

例 5-13　ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是<u>　(64)　</u>，选定的多路复用技术是<u>　(65)　</u>。(2015 年下半年真题 64、65)

(64) A. 10Mb/s　　B. 100Mb/s　　C. 20Mb/s　　D. 1Gb/s

(65) A. OFDM　　B. QPSK　　C. MIMO　　D. 64-QAM

解析：ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是 100Mb/s，选定的复用技术是正交频分复用(OFDM)。这是一种无线环境下的高速传输技术，其主要思想就是在频段内将给定信道分成许多正交子信道，在每个子信道上使用一个子载波进行调制，各子载波并行传输。OFDM 技术的优点是可以消除或减小信号波形间的干扰，对多径衰落和多普勒频移不敏感，提高了频谱利用率。

答案：(64) B　(65) A

例 5-14　4G 移动通信标准 TD-LTE 与 FDD-LTE 的区别是__(62)__。(2015 年上半年真题 62)

A. 频率的利用方式不同　　B. 划分上下行信道的方式不同

C. 采用的调制方式有区别　　D. 拥有专利技术的厂家不同

解析：TD-LTE 与 FDD-LTE 的区别不大，都属于 LTE 的分支。FDD(Frequency Division Duplexing)是频分双工，有两个独立的信道，一个用来向下传送信息，另一个用来向上传送信息。两个信道之间存在一个保护频段，以防止邻近的发射机和接收机之间产生相互干扰。而 TDD (Time Division Duplexing) 是时分双工，发射和接收信号是在同一频率信道的不同时隙中进行的，彼此之间采用一定的保证时间予以分离。

答案：A

5.4.3　同步练习

1. 在无线通信领域，现在主流应用的是第四代(4G)通信技术，其理论下载速率可达到 Mbps(兆比特每秒)。

A. 2.6　　B. 4　　C. 20　　D. 100

2. 一下哪个协议属于 WLAN 协议？________

A. 802.15　　B. 802.16　　C. 802.20　　D. 802.11

5.4.4　同步练习参考答案

1. D　　2. D

5.5　本 章 小 结

本章知识点在 2014 年的新大纲中是新增章节，从原先的局域网与城域网章节中分离出来。

本章主要介绍了无线局域网，除此之外新增了移动通信、无线个域网和无线城域网等当前主流技术。2014 年两次考试中已出现了相关的题目，新加的内容需要作为学习的重点。

无线局域网标准和 CSMA/CA 协议是重点，一般考试中都会出现。

本章相关知识点在历次考试中分布相对集中，分值在 5 分左右。根据往年的考题，本章的内容，要以典型例题为主线，抓住重点。本章每节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

5.6　达标训练题及参考答案

5.6.1　达标训练题

1. 2009 年发布的________标准可以将 WLAN 的传输速率由 4Mb/s 提高到 300～600Mb/s。

A. IEEE 802.11n　　B. IEEE 802.11a
C. IEEE 802.11b　　D. IEEE 802.11g

2. IEEE 802.11 标准定义的 Peer to Peer 网络是________。

A. 一种需要 AP 支持的无线网络
B. 一种不需要有线网络和接入点支持的点对点网络
C. 一种采用特殊协议的有线网络
D. 一种高速骨干数据网络

3. IEEE 802.11g 标准支持最高数据速率可达________ Mb/s。

A. 5　　B. 11　　C. 54　　D. 100

4. 下面关于 WLAN 安全标准 IEEE 802.11i 的描述中，错误的是________。

A. 采用了高级加密标准(AES)　　B. 定义了新的密钥交换协议(TKIP)
C. 采用 802.1x 实现访问控制　　D. 提供的加密方式为有线等价协议(WEP)

5. 关于无线局域网，下面叙述中正确的是________。

A. 802.11a 和 802.11b 都可以在 2.4GHz 频段工作
B. 802.11b 和 802.11g 都可以在 2.4GHz 频段工作
C. 802.11a 和 802.11b 都可以在 5GHz 频段工作
D. 802.11b 和 802.11g 都可以在 5GHz 频段工作

6. IEEE 802.11i 标准增强了 WLAN 的安全性。下面关于 802.11i 的描述中，错误的是________。

A. 加密算法采用高级数据加密标准(AES)
B. 加密算法采用对等保密协议(WEP)
C. 用 802.1x 实现了访问控制
D. 使用 TKIP 实现了动态的加密过程

7. IEEE 802.11 定义了无线局域网的两种工作模式，其中的__(1)__模式是一种点对点连接的网络，不需要无线接入点和有线网络的支持。IEEE 802.11g 的物理层采用了扩频技术，工作在__(2)__频段。

(1) A. Roaming　　B. Ad Hoc　　C. Infrastructure　　D. Diffuse IP
(2) A. 600MHz　　B. 800MHz　　C. 2.4GHz　　D. 19.2GHz

5.6.2　参考答案

1. A　　2. B　　3. C　　4. D　　5. B
6. B　　7. (1) B　(2) C

第 6 章　网络互连与互联网

大纲要求：

- 常见的网络互连设备(中继器、Hub、网桥、交换机、路由器、网关)的工作原理，以及与 OSI 的七层模型关系，广播域和冲突域。
- 多层交换技术：三层交换、四层交换、ATM+IP 交换、MPLS。
- 路由选择协议：路由获取方法、静态路由和动态路由的分类。
- 距离矢量路由算法：基本思想，RIP、IGRP 路由协议。
- 链路状态路由算法：基本思想，OSPF 的特点、分组类型、区域划分、分组的时间间隔，DR 和 BDR 的作用及选举。
- 外部网关路由协议：应用场合、BGP4 的特点及报文。

6.1　网络互连设备

6.1.1　考点辅导

1. 中继器

中继器工作在 OSI 模型的物理层，主要功能是对接收的信号进行再生和发送。中继器不解释也不改变接收到的数字信息，它只从接收的信号中分离出数字数据，存储起来，然后重新构造它并转发出去。再生的信号与接收的信号完全相同，并可以沿着另外的网段传输到远端。

以太网中对中继器的使用上限控制在 4 个，即最多由 5 个网段组成。而且中继器也不能把传输介质不同的网络连接在一起。

2. 网桥

网桥(Bridge)是一种连接局域网的网络互联设备，工作在数据链路层。网桥具有过滤帧的功能，通过分析帧地址字段，以决定是否把收到的帧转发到另一个网络段上。

当网桥收到一个帧时，并不是向所有端口转发此帧，而是先检查此帧的源地址和目的地址。如果目的地址和源地址不在同一个网段上，就把帧转发到另一个网段上；若两个地址在同一个网段上，则不转发。网桥的工作原理如图 6-1 所示。

(1) 在图 6-1 中，若工作站 H_1 向工作站 H_2 发送以太网帧，因工作站 H_2 与工作站 H_1 在同一个物理网段上，网桥对此帧进行过滤，不转发该帧。

(2) 若工作站 H_1 向工作站 H_4 发送以太网帧，网桥通过查找网桥表知道工作站 H_4 与网桥端口 2 对应，就将该帧从端口 2 转发。

(3) 若工作站 H_1 向工作站 H_7 发送以太网帧，而在网桥地址表中未找到关于工作站 H_7

的 MAC 地址与端口的对应关系，此时，网桥会把这个发往未知目的 MAC 地址的帧向除发送该帧的源端口外的其他所有端口进行转发。在这种情况下，网桥充当的实际上是集线器的角色，确保没有使信息停止传送。

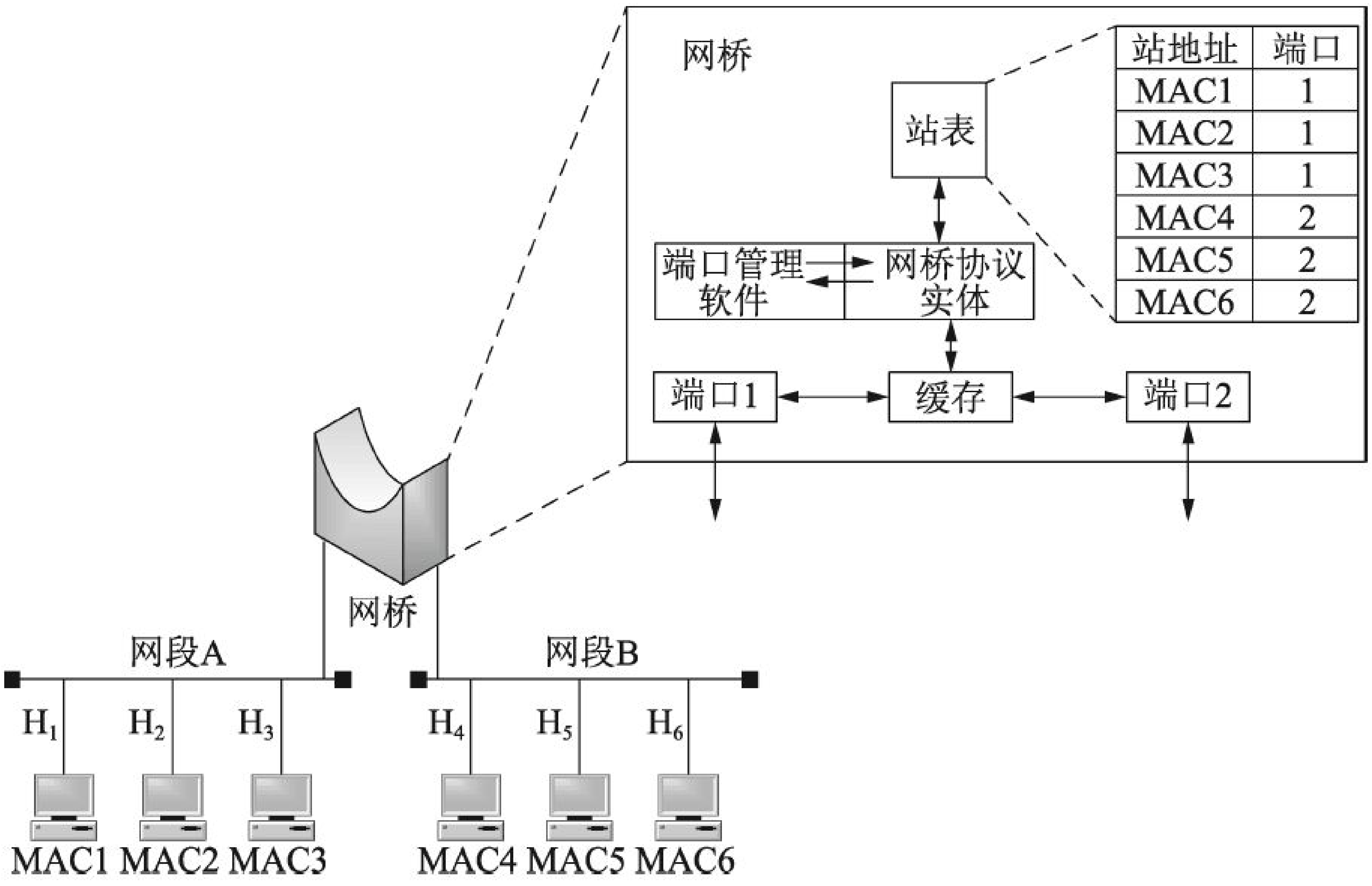


图 6-1　网桥的工作原理

网桥工作在 MAC 子层，只要两个网络 MAC 子层以上的协议相同，都可以用网桥互联。另外，网桥还可以连接不同传输介质的网络。

以太网中广泛使用的交换机是一种多端口网桥，每个端口可以连接一个局域网。

3. 路由器

路由器适合于连接复杂的大型网络，它工作在网络层，可以用于连接下面 3 层执行不同协议的网络，协议的转换由路由器完成，从而可消除网络层协议之间的差别。通过路由器连接的子网在网络层之上必须执行相同的协议。

相比于网桥，路由器的互联能力更强，可以执行复杂的路由选择算法。但路由器处理的信息量比网桥要多，因此处理速度比网桥慢。要注意的是，路由器是具有路由选择功能的网桥，路由器虽然能运行路由选择算法，但它不涉及第三层协议，仍工作在数据链路层。

4. 网关

网关是最复杂的网络互联设备，它用于连接网络层之上执行不同协议的子网，组成异构型的互联网。为了实现异构型设备之间的通信，网关要对不同的传输层、会话层、表示层和应用层协议进行翻译和变换。

由于工作复杂，因此用网关进行网络互联时效率比较低，而且透明性不好。因而网关往往用于针对某种特殊用途的专用连接。有时并不划分路由器和网关，而把网络层及其以上进行协议转换的互联设备统称为网关。

6.1.2 典型例题分析

例 6-1 集线器与网桥的区别是__(11)__。(2015 年下半年真题 11)

A. 集线器不能检测发送冲突，而网桥可以检测冲突

B. 集线器是物理层设备，而网桥是数据链路层设备

C. 网桥只有两个端口，而集线器是一种多端口网桥

D. 网桥是物理层设备，而集线器是数据链路层设备

解析：集线器是物理层设备，可视为一种特殊的中继器，用于扩大网络；网桥是数据链路层设备，用于连接两个局域网网段。确切地讲，网桥工作在 MAC 子层，只要两个网络的 MAC 子层以上的协议相同，都可以用网桥互连。

答案：B

例 6-2 以下关于网桥和交换机的区别的叙述中，正确的是__(13)__。(2015 年上半年真题 13)

A. 交换机主要是基于软件实现，而网桥是基于硬件实现的

B. 交换机定义了广播域，而网桥定义了冲突域

C. 交换机根据 IP 地址转发，而网桥根据 MAC 地址转发

D. 交换机比网桥的端口多，转发速度更快

解析：网桥用于连接两个局域网，工作在数据链路层。交换机是一种多端口的网桥。网桥可以是专门硬件设备，也可以由计算机加装的网桥软件来实现，这时计算机上会安装多个网络适配器(网卡)。网桥工作在数据链路层，将两个 LAN 连起来，根据 MAC 地址来转发帧，可以看作一个“低层的路由器”。

答案：D

6.1.3 同步练习

下面关于交换机的说法中，正确的是______。

A. 以太网交换机可以连接运行不同网络层协议的网络

B. 从工作原理上讲，以太网交换机是一种多端口网桥

C. 集线器是一种特殊的交换机

D. 通过交换机连接的一组工作站形成一个冲突域

6.1.4 同步练习参考答案

B

6.2 广域网互联

6.2.1 考点辅导

1. OSI 网络层内部结构

为了实现类型不同的子网互联，OSI 把网络层划分为 3 个子层：子网访问层、子网相关

层和子网无关层。

(1) 子网访问层对应于实际网络的第三层，它不一定符合 OSI 的网络层标准。如果两个实际网络的子网访问子层不同，则它们不能简单地互联。

(2) 子网相关层的作用是增强实际网络的服务，使其接近于 OSI 的网络层服务，两个不同类型的子网经过分别增强后可达到相同的服务水准。

(3) 子网无关层提供标准的 OSI 网络服务，它利用子网相关子层提供的功能，按照 OSI 网络层协议实现两个子网的互联。

2. 面向连接的网际互联

实现面向连接的网际互联的前提是子网提供面向连接的服务，这样可以用路由器连接两个或多个子网，路由器是每个子网的 DTE。当不同子网中的 DTE 要进行通信时，就通过路由器建立一条跨网络的虚电路。这种网际虚电路是通过路由器把两个子网中的虚电路级联起来实现的。如图 6-2 所示，主机 A 和主机 B 通过建立的虚电路传送信息。

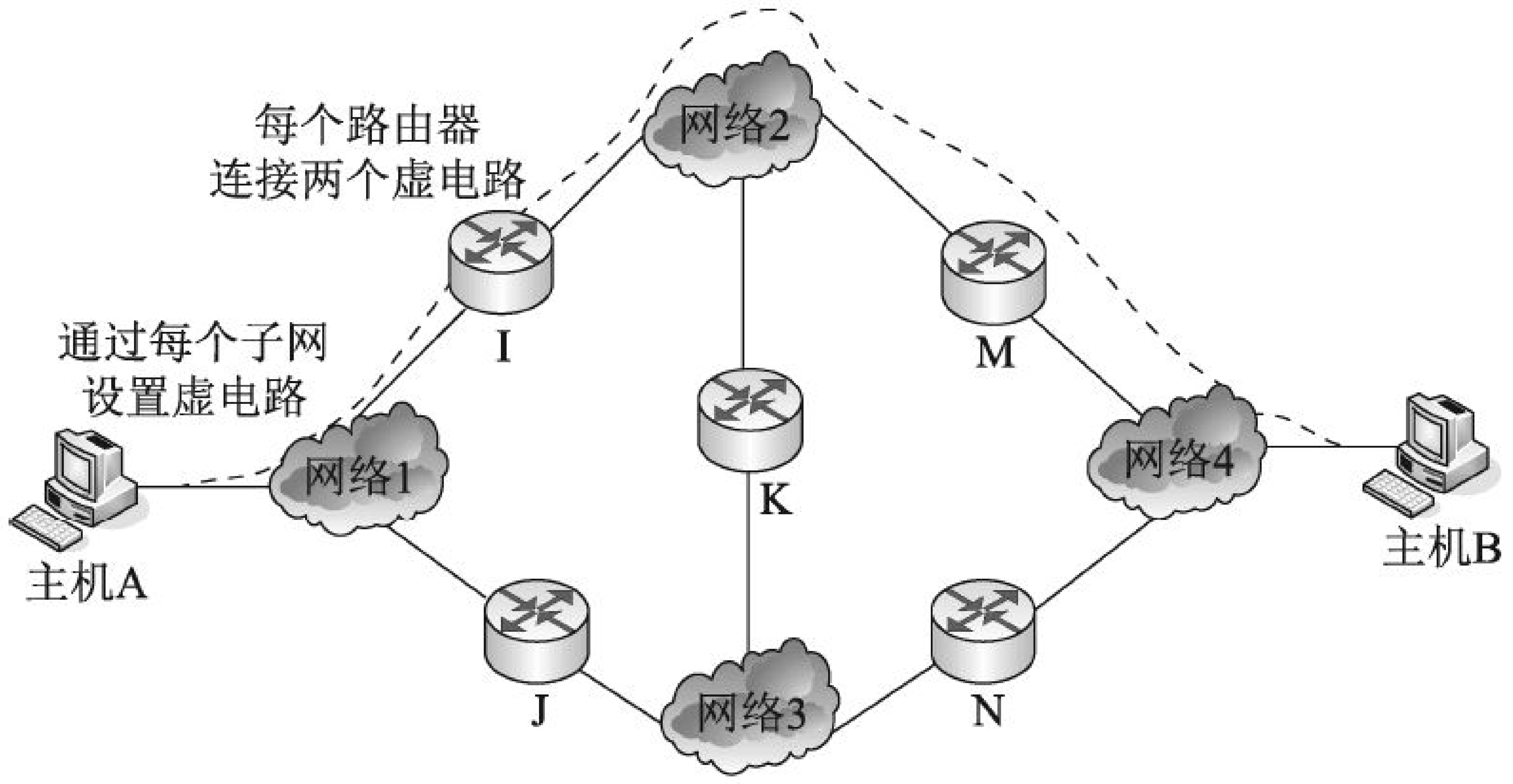


图 6-2　面向连接的解决方案

面向连接的解决方案要求互联网中的每一个物理网络都能提供面向连接的服务，但这样的要求在实际中是不现实的。

3. 无连接的网际互联

如果网络仍采用图 6-2 所示的拓扑结构，在无连接的方案中，主机 A 和主机 B 之间通信时不需要建立虚电路，数据单元在网络中分别独立传输，这些数据单元经过一系列的网络和路由器，最终到达目的节点。由于网络设备对每个数据单元的路由选择是独立进行的，因此不同的数据单元到达目的主机经过的路径可能不同。

目前，流行的互联网就是采用了面向无连接的解决方案。IP 是面向非连接的互联网络解决方案中最常用的协议。IP 是为 ARPAnet 研制的网际数据报协议，后来 ISO 以此为蓝本开发了无连接的网络协议(ConnectionLess Network Protocol，CLNP)。CLNP 与 IP 的功能十分相似，差别只在于个别细节和分组格式不同。

实际上，网际协议要解决的问题与网络层协议类似。在网际层提供路由信息的手段仍然是路由表。每个站或路由器都有一个网际路由表，表的每一行说明与一个目标站对应的

路由器地址。网际地址通常采用“网络.主机”的形式，其中网络部分是子网的地址编码，主机部分是子网中主机的地址编码。

6.2.2 典型例题分析

例 6-3 OSI 把网络层划分为 3 个子层，下列不属于该划分的是________。

A. 子网无关层　　B. 子网相关层　　C. 子网访问层　　D. 互联层

解析：OSI 把网络层划分为 3 个子层：子网无关层、子网相关层和子网访问层。

答案：D

6.2.3 同步练习

下列说法错误的是________。

A. 子网访问层对应于实际网络的第三层，它不一定符合 OSI 的网络层标准

B. 子网相关层的作用是增强实际网络的服务，使其接近于 OSI 的网络层服务，两个不同类型的子网经过分别增强后可达到相同的服务水准

C. 子网无关子层提供标准的 OSI 网络服务

D. 两个实际网络的子网访问子层不同时也可以进行简单的互联

6.2.4 同步练习参考答案

D

6.3 IP 协 议

6.3.1 考点辅导

6.3.1.1 IP 地址

一个 IP 地址由网络号和主机号两部分组成，由 4 字节共 32 位的数字串组成，这 4 字节通常用小数点分隔。每字节可用十进制表示，如 192.46.8.22。IP 地址也可以用二进制和十六进制表示。

1. IP 地址分类

IP 地址分为 5 类，如表 6-1 所示，其中 A、B、C 类是常用地址。

表 6-1　Internet 的 IP 地址空间容量

IP 地址类型	第一字节十进制范围	二进制固定最高位	二进制网络位数	网络数	二进制主机位数	主机数
A 类	0～127	0	8	126	24	$2^{24}-2$
B 类	128～192	10	16	2^{14}	16	$2^{16}-2$

续表

IP 地址类型	第一字节十进制范围	二进制固定最高位	二进制网络位数	网络数	二进制主机位数	主机数
C 类	192～223	110	24	2^{21}	8	2^8-2
D 类	224～239	1110	组播地址			
E 类	240～255	11110	保留给实验使用			

IP 地址除了标识一台主机外，还有几种具有特殊意义的形式。

(1) 本网络的本台主机。若一个 IP 地址由全 0 组成，即 0.0.0.0，表示在本网络上本台主机，当一台主机在运行引导程序但又不知道其 IP 地址时使用该地址。

(2) 本网络的某台主机。网络号各位全为“0”的 IP 地址，表示在这个网络中的特定主机。它用于一个主机向同网络中其他主机发送报文。

(3) 网络地址。主机号各位全为“0”的 IP 地址标识本网络的网络地址，不分配给任何主机。

(4) 直接广播地址(有时就简称为广播地址)。主机号各位全为“1”的 IP 地址，不分配给任何主机，它用于将一个分组发送给特定网络上的所有主机，即对全网广播。

(5) 受限(本地)广播地址。受限广播地址是 32 位全 1 的 IP 地址(255.255.255.255)。该地址用于主机配置过程中 IP 数据报的目的地址，此时，主机可能还不知道它所在网络的网络掩码，甚至连它的 IP 地址也不知道。在任何情况下，路由器都不转发目的地址为受限的广播地址的数据报，这样的数据报仅出现在本地网络中。

(6) 回送地址(Loopback Address)。A 类网络地址 127.X.X.X 是一个保留地址，用于网络软件测试以及本地进程间的通信。

如果一个组织不需要接入到因特网上，但需要在其网络上运行 TCP/IP 协议，最佳选择是使用私网地址，但 Internet 中路由器一般不转发目标地址为私网地址的数据包。私网地址如表 6-2 所示。

表 6-2　私网 IP 地址空间

类　型	网络地址	网 络 数
A 类	10.0.0.0	1
B 类	172.16.0.0～172.31.0.0	16
C 类	192.168.0.0～192.168.256.0	256

2. 子网划分和子网掩码

由于 IP 地址的分配是以“网络”为单位进行的，如果一个部门拥有 256 个用户接入 Internet，至少应该为该部门分配两个连续的 C 类网地址。很显然，这种分配制度导致了大量的 IP 地址资源的浪费。为了提高 IP 地址的使用效率，可采用借位的方式将一个网络划分为子网：从主机号最高位开始借位变为新的子网号，所剩余的部分仍为主机号。这使得 IP 地址的结构分为 3 部分：网络号、子网号和主机号。

引入子网划分技术后带来了一个重要问题，即主机路由和路由设备如何判断一个给定的 IP 地址是否已经进行了子网划分，从而能正确地从 IP 地址中分离出有效的网络标识。通

常，将引入子网划分技术前的 A、B、C 类地址称为有类别(Classful)的 IP 地址；将引入子网划分技术后的 IP 地址称为无类别(Classless)的 IP 地址，并因此引入子网掩码来描述 IP 地址中关于网络标识和主机号位数的组成情况。

子网掩码(Subnetmask)通常与 IP 地址配对出现，其功能是告知主机或路由设备，IP 地址的哪一部分代表网络号部分，哪一部分代表主机号部分。子网掩码使用与 IP 地址相同的编码格式，长 32 位，由一串 1 和跟随的一串 0 组成。子网掩码中的 1 对应于 IP 地址中的网络号(net-id)和子网号(subnet-id)，而子网掩码中的 0 对应于 IP 地址中的主机号(host-id)。要得到网络或子网地址，只需将 IP 地址和子网掩码按位进行“与”运算即可。

子网掩码有两种表示方法。

(1) 用点分十进制表示法表示，如 256.256.256.0、256.256.256.240 等。

(2) 在 IP 地址后加一个“/网络号和子网号的位数”。例如，210.46.12.58/28 就表示该 IP 地址的网络号(net-id)和子网号(subnet-id)共占用 28 位，主机号占用 32−28=4 位，如果用点分十进制表示法表示，则子网掩码为 256.256.256.240，其二进制表示为

11111111 11111111 11111111 11110000

采用子网掩码是对网络编址的有益补充，但是还存在着一些缺陷，如划分的子网中较小的会浪费许多地址。为了解决这个问题，避免任何可能的地址浪费，就出现了可变长子网掩码(Variable Length Subnetwork Mask，VLSM)的编址方案。VLSM 允许一个网络使用不同的网络掩码以适应不同规模的子网要求。

6.3.1.2 IP 协议的操作

下面首先讨论 IP 协议的主要操作。

1. 数据报生存期

如果使用了动态路由选择算法，或者允许在数据报旅行期间改变路由决定，则有可能造成回路。最坏的情况是数据报在网际中无休止地巡回，不能到达目的地并浪费大量的通信资源。

解决这个问题的简单办法是规定数据报有一定的生存期，生存期的长短以它经过的路由器的多少计数。每经过一个路由器，计数器加 1，计数器超过一定的计数值，数据报就被丢弃。

当然也可以用一个全局的计时时钟记录数据报的生存期。在这种方案下，生成数据报的时间被记录在报头中，每个路由器查看这个记录，决定是继续转发还是丢弃它。

2. 分段和重装配

每个网络可能规定了不同的最大分组长度。当分组在互联网中传送时可能要进入一个最大分组长度较小的网络，这时需要对它进行分段，这又引出了新的问题：在哪里对它进行重装配？

一种办法是在目的地进行装配。但这样只会把数据报越分越小，即使后续子网允许较大的分组通过，但由于途中的短报文无法装配，从而使效率下降。

另一种办法是允许中间的路由器进行组装，这种方法也有缺点。首先是路由器必须提供重装配缓冲区，并且要设法避免重装配死锁；其次是由一个数据报分出的小段都必须经

过同一个出口路由器，才能再行组装，这就排除了使用动态路由选择算法的可能性。

关于分段和重装配问题的讨论还在继续，已经提出了各种各样的方案。下面介绍在 DOD 和 ISO IP 协议中使用的方法，这个方法有效地解决了以上提出的部分问题。

IP 协议使用了 4 个字段处理分段和重装配问题。一个是报文 ID 字段，它唯一地标识了某个站某个协议层发出的数据。在 DOD(美国国防部)的 IP 协议中，ID 字段由源站和目标站地址、产生数据的协议层的标识符以及该协议层提供的顺序号组成。第二个字段是数据长度，即字节数。第三个字段是偏置值，即分段在原来数据报中的位置，以 8 字节(64 位)的倍数计数。最后是 M 标志，表示是否为最后一个分段。

当一个站发出数据报时对长度字段的赋值等于整个数据字段的长度，偏置值为 0，M 标志置 False(用 0 表示)。如果一个 IP 模块要对该报文分段，则按以下步骤进行。

(1) 对数据块的分段必须在 64 位的边界上划分，因而除最后一段外，其他段长都是 64 位的整数倍。

(2) 对得到的每一分段都加上原来数据报的 IP 头，组成短报文。

(3) 每一个短报文的长度字段置为它包含的字节数。

(4) 第一个短报文的偏置值置为 0，其他短报文的偏置值为它前边所有报文长度之和(字节数)除以 8。

(5) 最后一个报文的 M 标志置为 0(False)，其他报文的 M 标志置为 1(True)。

表 6-3 给出一个分段的例子。

表 6-3　数据报分段的例子

项　目	长　度	偏 置 值	M 标 志
原来的数据报	475	0	0
第一个分段	240	0	1
第二个分段	235	30	0

重装配的 IP 模块必须有足够大的缓冲区。整个重装配序列以偏置值为 0 的分段开始，以 M 标志为 0 的分段结束，全部由同一 ID 的报文组成。

数据报服务中可能发生有一个或多个分段不能到达重装配点的情况。为此，采用两种对策应付这种意外。一种是在重装配点设置一个本地时钟，当第一个分段到达时把时钟置为重装配周期值，然后递减，如果在时钟值减到零时还没等齐所有的分段，则放弃重装配。另一种对策与前面提到的数据报生存期有关，目标站的重装配功能在等待的过程中继续计算已到达的分段的生存期，一旦超过生存期，就放弃重装配，丢弃已到达的分段。显然，这种计算生存期的办法必须有全局时钟的支持。

3. *差错控制和流控*

无连接的网络操作不保证数据报的成功递交，当路由器丢弃一个数据报时，要尽可能地向源点返回一些信息。源点的 IP 实体可以根据收到的出错信息改变发送策略或者把情况报告上层协议。丢弃数据报的原因可能是超过生存期、网络拥挤、FCS 校验出错等。在最后一种情况下可能无法返回出错信息，因为源地址字段已不可辨认了。

路由器或接收站可以采用某种流控机制来限制发送速率。由于这里谈的是无连接的数

据报服务，因此可采用的流控机制是很有限的。最好的办法也许是向其他站或路由器发送专门的流控分组，使其改变发送速率。

6.3.1.3 IP 协议的数据单元

目前因特网上广泛使用的 IP 协议为 IPv4，其数据报格式如图 6-3 所示。IPv4 的设计目标是提供无连接的数据报尽力投递服务。

<table>
<tr><td>0</td><td>4</td><td>8</td><td>16</td><td></td><td>31</td></tr>
<tr><td>版本号</td><td>IP头长度</td><td>服务类型</td><td colspan="3">IP数据报长度</td></tr>
<tr><td colspan="3">标识符</td><td>标志</td><td colspan="2">段偏移</td></tr>
<tr><td colspan="2">生存期</td><td>协议</td><td colspan="3">报头校验和</td></tr>
<tr><td colspan="6">源IP地址</td></tr>
<tr><td colspan="6">宿IP地址</td></tr>
<tr><td colspan="5">IP选项</td><td>填充域</td></tr>
<tr><td colspan="6">数据域</td></tr>
</table>

图 6-3　IPv4 数据报格式

IP 数据报包括 IP 数据报报头和数据域两部分，报头主要包含数据报传输时所用的控制信息，数据域携带用户希望传输的数据信息。

- 版本号：说明对应 IP 协议的版本号(此处取值为 4)。
- IP 头长度：以 32 位字为单位的 IP 数据报报头的长度。
- 服务类型：说明本数据报对传输网络的性能要求，或者指导路由器选择适合的传输网络。前 3 位表示本数据报的优先级(取值为 0 表示一般数据，取值为 7 表示网络控制信息)；第四～六位分别为延迟(D)、吞吐量(T)和可靠性(R)标志位；最后两位保留未用。
- IP 数据报长度：说明整个 IP 数据报的长度，以字节为单位，最大值为 65 535。
- 标识符：唯一地标识该份 IP 数据报；IP 模块提供尽力投递的服务，在 IP 数据报投递的过程中，可能执行数据报分段的工作，将一个体积较大的数据报划分为若干个小的数据报。为了便于收方 IP 模块的组装，所有小数据报的标识符域具有相同的值。
- 标志：说明本数据报是否允许分段。本域共占 3 位，从左至右第一位保留未用，第二位(DF)表示是否允许分段，第三位(MF)表示本分段是否为最后一段。
- 段偏移：说明本数据报分段在整个数据报中的起始位置；由于段偏移域共占 13 位，表示源发节点发送的 IP 数据报最多允许有 8192 个分段。
- 生存期：说明本 IP 数据报在网络中允许停留的时间。为了避免 IP 数据报在网络中无限制地转发，设置了本字段。通常本字段由源发端设置，并且每经过一个路由器(分析 IP 数据报)，数值减 1；结果为 0，则丢弃本数据报。
- 协议：说明其上层用户协议，如 TCP、UDP 等。
- 报头校验和：用于路由器检测 IP 数据报报头的正确性。该域的值在 IP 数据报途经的每个路由器上重新生成，并由下一跳的路由器验证。IP 模块丢弃报头出错的数据报，并通过 ICMP(因特网控制消息协议)告知发送方。
- 源/宿 IP 地址：填写本 IP 数据报的发送方和接收方的 IP 地址。

- IP 选项：用于对 IPv4 的功能扩充。
- 填充域：保证整个 IP 数据报报头的长度为 32 位字的整数倍。如果报头长度不是 32 位的整数倍，则需要在填充域中加 0 凑齐。

6.3.2　典型例题分析

例 6-4　IP 数据报经过 MTU 较小的网络时需要分片。假设一个大小为 1500 的报文分为 2 个较小报文，其中一个报文大小为 800 字节，则另一个报文的大小至少为 (22) 字节。(2017 年下半年真题 22)

A. 700　　B.720　　C.740　　D. 800

解析：报文大小为 800 字节，至少有 20 字节的首部，则数据部分为 800−20=780 字节，另一个报文的数据部分(1500−20)−780=700，再加上 20 字节的首部，其大小为 720 字节。实际上各分片的报文要为 8b 的整数倍。

答案：B

例 6-5　下面的地址中，可以分配给某台主机接口的地址是 (54) 。(2017 年下半年真题 54)

A. 224.0.0.23　　B. 220.168.124.127/30

C. 61.10.191.255/18　　D. 192.114.207.78/27

解析：A 选项为组播地址。B 选项 220.168.127.0111 1111，C 选项 61.10.1011 1111.1111 1111，主机号均为全 1，不分配给任何主机，属于广播地址。有效的主机地址主机号位非全 0 和非全 1。

答案：D

例 6-6　以下 IP 地址中，属于网络 201.110.12.224/28 的主机 IP 是 (55) 。(2017 年下半年真题 55)

A. 201.110.12.224　　B. 201.110.12.238

C. 201.110.12.239　　D. 201.110.12.240

解析：201.110.12.224/28 即 201.110.12.11100000，它的可用主机地址范围是：201.110.12.225～201.110.12.238。

答案：B

例 6-7　某单位 IP 地址需求数如下表所示，给定地址 192.168.1.0/24，按照可变长子网掩码的设计思想，部门 3 的子网掩码为 (52) 。(2017 年上半年真题 52)

二级单位名称	IP 地址需求数
部门 1	100
部门 2	50
部门 3	30
部门 4	10
部门 5	10

A. 255.255.255.128　　B. 255.255.255.192

C. 255.255.255.224　　　　D. 255.255.255.240

解析：首先 192.168.1.0/24 分成两个子网，一个给部门 1 用，另外一个继续划分为两个子网，一个给部门 2 用，另一个继续划分子网，一个给部门 3 用，剩下的依旧划分子网，给部门 4、5 用。因此部门 3 的子网掩码是 255.255.255.224。

答案：C

例 6-8　假设某单位有 1000 台主机，则至少需分配__(53)__个 C 类网络，若分配的超网号为 202.25.64.0，则地址掩码是__(54)__。(2017 年上半年真题 53、54)

(53) A .4　　B. 8　　C. 12　　D. 16

(54) A. 255.255.224.0　　B. 255.255.240.0　　C. 255.255.248.0　　D. 255.255.252.0

解析：一个 C 类网络最多有 254 台主机，1000 台主机需要 4 个 C 类网络。容纳这 1000 台主机的超网掩码是 255.255.252.0。

答案：(53) A　(54)D

例 6-9　在网络最多有 101.113.10.0/29 中，能接收到目的地址是 101.113.10.7 的报文的主机数最多有__(55)__个。(2017 年上半年真题 55)

A.　1　　B. 3　　C. 5　　D. 6

解析：网络 101.113.10.0/29 中，可用主机范围是 101.113.10.1～101.113.10.6，主机数是 6。

答案：D

例 6-10　ISP 分配给某公司的地址块为 199.34.76.64/28，则该公司得到的 IP 地址数是__(51)__。(2016 年下半年真题 51)

A. 8　　B. 16　　C. 32　　D. 64

解析：网络位 28 位，主机位 4 位。IP 地址数为 2^4=16。

答案：B

例 6-11　下面 4 个主机地址中属于网络 110.17.200.0/21 的地址是__(53)__。(2016 年下半年真题 53)

A. 110.17.198.0　　B. 110.17.206.0

C.110.17.217.0　　D. 110.17.224.0

解析：110.17.200.0/21=110.107.11001000.0。主机号 11 位，其范围为 110.17.11001 000.0～110.17.11001 111.255，4 个选项中只有 B 项属于该范围。

答案：B

例 6-12　下面 4 个主机地址中属于网络 220. 115. 200. 0/21 的地址是__(51)__。(2016 年上半年真题 51)

A. 220.115.198.0　　B. 220.115.206.0

C. 220.115.217.0　　D. 220.115.224.0

解析：地址 220.115.198.0 的二进制形式是 1101 1100.0111 0011.1100 0110.0000 0000

地址 220.115.206.0 的二进制形式是 1101 1100.0111 0011.1100 1110.0000 0000

地址 220.115.217.0 的二进制形式是 1101 1100.0111 0011.1101 1001.0000 0000

地址 220.115.224.0 的二进制形式是 1101 1100.0111 0011.1110 0000.0000 0000

地址 220.115.200.0/21 的二进制形式是 1101 1100.0111 0011.1100 1000.0000 0000

所以与第二项匹配。

答案：B

例 6-13　采用可变长子网掩码可以把大的网络分成小的子网，例如把 A 类网络 60.15.0.0/16 分为两个子网，假设第一个子网为 60.15.0.0/17，则另一个子网为<u>　(52)　</u>。(2015 年下半年真题 52)

A. 60.15.1.0/17　　B. 60.15.2.0/17

C. 60.15.100.0/17　　D. 60.15.128.0/17

解析：把 A 类网络 60.15.0.0/17 分为两个子网，应该拿出 1 位主机进行子网划分，那么划分的两个子网分别是 60.15.0000 0000 0000 0000/17 和 60.15.1000 0000 0000 0000/17。

答案：D

例 6-14　假设用户 X 有 4000 台主机，则必须给他分配<u>　(53)　</u>个 C 类网络。如果为其分配的网络号为 196.25.64.0，则给该用户指定的地址掩码为<u>　(54)　</u>。(2015 年下半年真题 53、54)

(53) A. 4　　B. 8　　C. 10　　D. 16

(54) A. 255.255.255.0　　B. 255.255.250.0

C. 255.255.248.0　　D. 255.255.240.0

解析：C 类网络的主机号是 8 位，可容纳 254 台主机，现在用户 X 有 4000 台主机，则必须给他分配 C 类网络数目为 4000/254=15.7，所以给其分配 16 个 C 类网络。如果为其分配的网络号为 196.25.64.0，给用户指定的地址掩码中 0 的个数只要保证有 12 个，因为 $2^{12}-2=4096-2=4094$。所以选择答案 D，255.255.240.0 子网掩码中的 0 的个数是 12 个。

答案：(53) D　(54) D

例 6-15　如果指定的地址掩码是 255.255.254.0，则有效的主机地址是<u>　(52)　</u>。(2015 年上半年真题 52)

A. 126.17.3.0　　B. 174.15.3.255

C. 20.15.36.0　　D. 115.12.4.0

解析：由地址掩码 255.255.254.0 可知，IP 地址的前 23 位对应网络号，后 9 位对应主机号。选项 B 的主机号部分全为 1，表示广播地址；选项 C 和 D 中的地址后 9 位都为 0，为网络地址。

答案：A

6.3.3　同步练习

1.　以下地址中属于自动专用 IP 地址(APIPA)的是________。

A. 224.0.0.1　　B. 127.0.0.1　　C. 192.168.0.1　　D. 169.254.1.15

2.　公司得到一个 B 类网络地址块，需要划分成若干个包含 1000 台主机的子网，则可以划分成________个子网。

A. 100　　B. 64　　C. 128　　D. 500

3.　IP 地址 202.117.17.254/22 是什么地址？________

A. 网络地址　　B. 全局广播地址　　C. 主机地址　　D. 定向广播地址

4.　下列选项中，不属于网络 202.113.100.0/21 的地址是________。

A.202.113.102.0　B. 202.113.99.0　C. 202.113.97.0　D. 202.113.95.0

5. IP 地址块 112.56.80.192/26 包含了 __(1)__ 个主机地址，不属于这个网络的地址是 __(2)__。

(1) A. 15　B. 32　C. 62　D. 64

(2) A. 112.56.80.202　B. 112.56.80.191

C. 112.56.80.253　D. 112.56.80.195

6. 下面的地址中属于单播地址的是________。

A. 125.221.191.255/18　B. 192.168.24.123/30

C. 200.114.207.94/27　D. 224.0.0.23/16

6.3.4 同步练习参考答案

1. D　2. B　3. C　4. D　5. (1) C　(2) B　6. C

6.4 ICMP 协议

6.4.1 考点辅导

ICMP(因特网控制报文协议)与 IP 协议同属于网络层，用于传送有关通信问题的消息。例如，数据报不能到达目标站，路由器没有足够的缓存空间，或路由器向发送主机提供最短路径信息等。ICMP 报文封装在 IP 数据报中传送，因而不保证能可靠地提交。ICMP 报文有 11 种之多。报文中的类型字段表示 ICMP 报文的类型。

下面简要解释 ICMP 各类报文的含义。

(1) 目标不可到达(类型 3)。如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文；另一种情况是目标主机找不到有关的用户协议或上层服务访问点，也会返回这种报文。出现这种情况的原因可能是 IP 头中的字段不正确；或是数据报中说明的源路由无效；也可能是路由器必须把数据报分段，但 IP 头中的 D 标志已置位。

(2) 超时(类型 11)。路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时间内无法完成重装配，则向源端返回这种报文。

(3) 源抑制(类型 4)。这种报文提供了一种流量控制的初等方式。如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑制报文，这时源主机必须减小发送速率。另一种情况是系统的缓冲区已用完，并预感到行将发生拥挤，则发出源抑制报文。但是与前一种情况不同的是，所涉及的数据报尚能提交给目标主机。

(4) 参数问题(类型 12)。如果路由器或主机判断出 IP 头中的字段或语义出错，则返回这种报文，报文头中包含一个指向出错字段的指针。

(5) 路由重定向(类型 5)。路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。例如，路由器 R1 收到本地网络上的主机发来的数据报，R1 检查它的路由表，发

现要把数据报发往网络 X，必须先转发给路由器 R2，而 R2 又与源主机在同一网络中。于是 R1 向源主机发出路由重定向报文，把 R2 的地址告诉它。

(6) 回声(请求/响应，类型 8/0)。用于测试两个节点之间的通信线路是否畅通。收到回声请求的节点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 ping 程序就是这样工作的。

(7) 时间戳(请求/响应，类型 13/14)。用于测试两个节点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。这种应答过程如果结合强制路由的数据报实现，则可以测量出指定线路上的通信延迟。

(8) 地址掩码(请求/响应，类型 17/18)。主机可以利用这种报文获得它所在的局域网的子网掩码。首先主机广播地址掩码请求报文，同一局域网上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。了解子网掩码可以判断出数据报的目标节点与源节点是否在同一局域网中。

6.4.2　典型例题分析

例 6-16　当站点收到“在数据包组装期间生存时间为 0”的 ICMP 报文，说明 __(60)__ 。(2017 年下半年真题 60)

A. 回声请求没得到响应　　　　B. IP 数据报目的网络不可达

C. 因为拥塞丢弃报文　　　　　D. 因 IP 数据报部分分片丢失，无法组装

解析：TTL 通常表示包在被丢弃前最多能经过的路由器个数。当计数到 0 时，路由器决定丢弃该包，并发送一个 ICMP 报文给最初的发送者。TTL 值减为 0，说明在网络上经历很多跳之后依旧没有到达目的网络。

答案：B

例 6-17　关于 ICMP 协议，下面的论述中正确的是 __(14)__ 。(2015 年下半年真题 14)

A. 通过 ICMP 可以找到与 MAC 地址对应的 IP 地址

B. 通过 ICMP 可以把全局 IP 地址转换为本地 IP 地址

C. ICMP 用于动态分配 IP 地址

D. ICMP 可传送 IP 通信过程中出现的错误信息

解析：ICMP(Internet Control Message Protocol)是 TCP/IP 协议簇的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。

答案：D

6.4.3　同步练习

ICMP 协议属于因特网中的 __(1)__ 协议，ICMP 数据单元封装在 __(2)__ 中传送。

(1) A. 数据链路层　　B. 网络层　　C. 传输层　　D. 会话层

(2) A. 以太帧　　B. TCP 段　　C. UDP 数据报　　D. IP 数据报

6.4.4 同步练习参考答案

(1) B (2) D

6.5 TCP协议和UDP协议

6.5.1 考点辅导

IP 协议提供不可靠、无连接和尽力投递的服务，构成了因特网数据传输的基础。以此为基础，TCP 协议软件增加了确认—重发、滑动窗口和复用/解复用等机制。

1. TCP 协议的特性

TCP 协议在 IP 协议软件提供服务的基础上，支持面向连接的、可靠的、面向流的投递服务。

1) 面向流的投递服务

应用程序之间传输的数据可被视为无结构的字节流(或位流)，流投递服务保证收发的字节顺序完全一致。

2) 面向连接的投递服务

流传输之前，TCP 收发模块之间需建立连接(类似虚电路)，其后的 TCP 报文在此连接基础上传输。TCP 连接报文通过 IP 数据报进行传输，由于 IP 数据报的传输导致 ARP 地址映射表的产生，从而保证了后继的 TCP 报文可以具有相同的路径。

3) 可靠的传输服务

发送方 TCP 模块在形成 TCP 报文的同时，形成一个“累计核对”。“累计核对”类似于校验和，并随同 TCP 报文一起传输。接收方 TCP 模块根据该校验和判断传输的正确性：如果传输不正确，接收方简单地丢弃该 TCP 报文；否则进行应答。发送方如果在规定的时间内未能获得应答报文，则自动进行重传动作。

4) 缓冲传输

为了保证数据传输的效率，TCP 模块提供强制性传输(立即传输)和缓冲传输两种手段。缓冲传输允许将应用程序的数据流积累到一定的体积，形成报文，再进行传输。

5) 全双工传输

TCP 模块之间可以进行全双工的数据流交换。

6) 流量控制

TCP 模块提供滑动窗口机制，支持收发 TCP 模块之间的端到端流量控制。

2. TCP 端口和连接

TCP 模块以 IP 模块为传输基础，同时又可向多种应用程序提供传输服务。为了能够区分出对应的应用程序，引入了 TCP 端口的含义。

TCP 端口类似于 OSI 中传输层服务访问点，与一个 16 位的整数值相对应，该整数值也被称为 TCP 端口号。需要服务的应用进程与某个端口号进行连接，此时，TCP 模块就可以通过该 TCP 端口与应用进程通信。

由于 IP 地址可以对应到因特网中的某台主机，而 TCP 端口号可对应到主机上的某个应用进程，因此，TCP 模块采用 IP 地址和端口号的对偶来标识 TCP 连接的端点。一条 TCP 连接实质上对应了一对 TCP 端点。

3. TCP 窗口机制

TCP 的特点之一是提供体积可变的滑动窗口机制，支持端到端的流量控制。TCP 的窗口以字节为单位进行调整，以适应接收方的处理能力。处理过程如下。

(1) TCP 连接阶段，双方协商窗口尺寸，同时接收方预留数据缓存区。

(2) 发送方根据协商的结果，发送符合窗口尺寸的数据字节流，并等待对方的确认。

(3) 接收方根据当前的处理能力，调整接收窗口的尺寸，并在确认中告知发送方。

(4) 发送方根据确认信息，改变窗口的尺寸，增加或者减少发送未得到确认的字节流中的字节数。调整过程包括：如果出现发送拥塞，则应将发送窗口缩小为原来的一半，同时将超时重传的时间间隔扩大一倍。

TCP 的窗口机制和确认保证了数据传输的可靠性和流量控制。

4. UDP

UDP 是 TCP/IP 协议簇中等同于 TCP 的通信协议，其差异在于：UDP 直接利用 IP 进行 UDP 数据报的传输，因此 UDP 提供的是无连接、不可靠的数据报投递服务。

UDP 常用于数据量较少的数据传输。例如，域名系统中域名地址/IP 地址的映射请求和应答采用 UDP 进行传输，以减少 TCP 连接的过程，提高工作效率。

当使用 UDP 传输信息流时，用户负责解决排序、差错确认等问题。

6.5.2　典型例题分析

例 6-18　相比于 TCP，UDP 的优势为__(20)__。(2017 年下半年真题 20)

A. 可靠传输　　B. 开销较小　　C. 拥塞控制　　D. 流量控制

解析：UDP 是无连接、不可靠的传输，其优势为简单、效率高、开销小。

答案：B

例 6-19　主机甲向主机乙发送了一个 TCP 连接建立请求，主机乙给主机甲的响应报文中，标志字段正确的是__(24)__。(2017 年下半年真题 24)

A. SYN=1，ACK=1，FIN=0　　B. SYN=1，ACK=1，FIN=1

C. SYN=0，ACK=1，FIN=0　　D. SYN=1，ACK=0，FIN=0

解析：TCP 三次握手中，对 TCP 连接请求的响应应答为 SYN=1，ACK=1，FIN=0(代表终止 TCP 连接)。

答案：A

例 6-20　下面的应用中，__(38)__基于 UDP 协议。(2017 年下半年真题 38)

A. HTTP　　B. Telnet　　C. DHS　　D. FTP

解析：HTTP、FTP、Telnet 都是基于 TCP 协议的。

答案：C

例 6-21 主机甲向主机乙发送一个 TCP 报文段，SYN 字段为“1”，序列号字段的值为 2000，若主机乙同意建立连接，则发送给主机甲的报文段可能为 (22) ；若主机乙不同意建立连接，则 (23) 字段置“1”。(2017 年上半年真题 22、23)

(22) A. (SYN=1，ACK=1，seq=2001，ack=2001)

B. (SYN=1，ACK=0，seq=2000，ack=2000)

C. (SYN=l，ACK=0，seq=2001，ack=2001)

D. (SYN=0，ACK=1，seq=2000，ack=2000)

(23) A. URG　　B. RST　　C. PSH　　D. FIN

解析：主机乙同意建立连接后发回确认包(ACK)应答。即 SYN 标志位和 ACK 标志位均为 1。同时，将确认序号(Acknowledgement Number)设置为客户的序列号字段的值加 1，即 2001。FIN 表示连接终止。

答案：(22) A　(23) D

例 6-22 主机甲和主机乙建立一条 TCP 连接，采用慢启动进行拥塞控制，TCP 最大段长度为 1000 字节。主机甲向主机乙发送第一个段并收到主机乙的确认，确认段中接收窗口大小为 3000 字节，则此时主机甲可以向主机乙发送的最大字节数是 (24) 字节。(2017 年上半年真题 24)

A. 1000　　B. 2000　　C. 3000　　D. 4000

解析：慢启动进行拥塞控制算法如下。

MSS 数值：收发双方协商通信时每一个报文段所能承载的最大数据长度。所以 MSS=1000。

慢启动拥塞控制：每当收到一个 ACK，cwnd 呈线性上升。每当过了一个 RTT(发送报文到收到确认报文)，则 cwnd 呈指数上升。

主机甲发送报文段 M1 时，设置发送窗口 cwnd=MSS。主机甲向乙发送第一个报文段。

当主机甲收到报文段 K1 确认，则发送窗口 cwnd=cwnd+MSS，即 cwnd=2MSS，主机甲可以向乙发送报文段 M2、M3。

当主机甲收到报文段 K2、K3 确认，则发送窗口 cwnd=cwnd+2MSS，即 cwnd=4MSS，当前主机甲可以向乙发送报文段 M4、M5、M6、M7。

当主机甲收到报文段 K4、K5、K6、K7 确认，则发送窗口 cwnd=cwnd+4MSS，即 cwnd=8MSS，当前主机甲可以向乙发送报文段 M8～M15。

发送方窗口的上限值=Min[rwnd，cwnd]

因此当主机甲收到第一个报文段确认后，准备发送报文段时，cwnd=2MSS=2000。故甲可以发送最大 2000 字节。

答案：B

例 6-23 TCP/IP 网络中的 (13) 实现应答、排序和流控功能。(2016 年下半年真题 13)

A. 数据链路层　　B. 网络层　　C. 传输层　　D. 应用层

解析：传输层提供应用程序间的通信，包括格式化信息流，提供可靠传输。

答案：C

例 6-24　下面的应用层协议中通过 UDP 传送的是__(21)__。(2016 年下半年真题 21)

A. SMTP　　B. TFTP　　C. POP3　　D. HTTP

解析：TFTP 是简单文件传输协议，传输层的承载协议是 UDP。

答案：B

例 6-25　在建立 TCP 连接过程中，出现错误连接时，__(35)__标志字段置“1”。(2016 年下半年真题 35)

A. SYN　　B. RST　　C. FIN　　D. ACK

解析：复位 RST 为 1 时，说明 TCP 连接出现严重错误，需要释放连接，重新建立。

TCP 的标志字段(6 位)：表示各种控制信息。

URG：紧急指针有效。

ACK：应答顺序号有效。

PSH：推进功能有效。

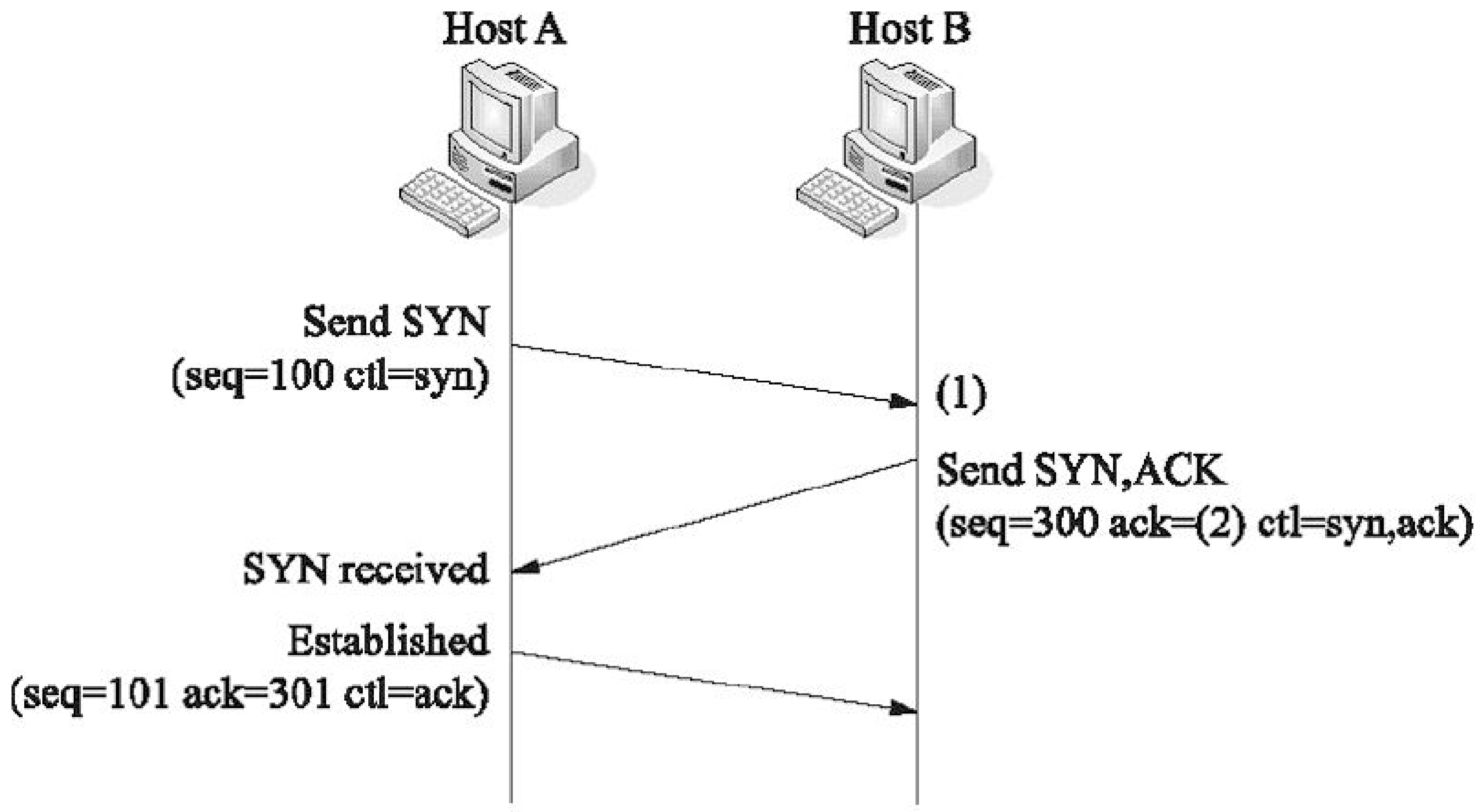
RST：连接复位为初始状态，通常用于连接故障后的恢复。

SYN：对顺序号同步，用于连接的建立。

FIN：数据发送完，连接可以释放。

答案：B

例 6-26　下图中主机 A 和主机 B 通过三次握手建立 TCP 连接，图中(1)处的状态是__(20)__，图中(2)处的数字是__(21)__。(2015 年下半年真题 20、21)



(20) A. SYN received　　B. Established　　C. Listen　　D. FIN wait

(21) A. 100　　B. 101　　C. 300　　D. 301

解析：TCP 三次握手流程如下。

(1) A 的 TCP 客户进程首先向 B 发出连接请求报文段，这时首部中的同步位 SYN=1，同时选择一个初始序号 seq=x。TCP 规定，SYN 报文段(SYN=1 的报文段)不能携带数据，但要消耗一个序号。这时候，客户进程进入同步已发送状态。

(2) B 收到这个连接请求之后，如同意建立连接，则向 A 发送确认。在确认报文段中应把 SYN 位和 ACK 位都置 1，确认号是 ack=x+1，同时也为自己选择一个初始序号 seq=y。注意，这个报文段也不能携带数据，但同样要消耗一个序号。这时 TCP 服务器进程进入同步收到状态。

(3) TCP客户进程收到B的确认后，还要向B给出确认，确认报文段的ACK置1，确认号ack=y+1，则自己的序号seq=x+1。TCP协议规定，ACK报文段可以携带数据，但如果不携带数据则不消耗序号。在这种情况下，下一个数据报文段的序号依然是seq=x+1。这时，TCP连接已经建立，A进入已建立连接状态。

答案：(20) A　(21) B

例 6-27　TCP使用的流量控制协议是__(22)__。(2015年下半年真题22)

A. 固定大小的滑动窗口协议　　B. 后退N帧的ARQ协议

C. 可变大小的滑动窗口协议　　D. 停等协议

解析：TCP使用一种窗口(Window)机制来控制数据流。TCP的窗口以字节为单位进行调整，以适应接收方的处理能力。处理过程如下。

(1) TCP连接阶段，双方协商窗口尺寸，同时接收方预留数据缓存区。

(2) 发送方根据协商的结果，发送符合窗口尺寸的数据字节流，并等待对方的确认。

(3) 发送方根据确认信息，改变窗口的尺寸，增加或者减少发送未得到确认的字节流中的字节数。调整过程包括：如果出现发送拥塞，发送窗口缩小为原来的一半，同时将超时重传的时间间隔扩大一倍。

答案：C

6.5.3　同步练习

如果一个TCP连接处于ESTABLISHED状态，这是表示________。

A. 已经发出了连接请求　　B. 连接已经建立

C. 处于连接监听状态　　D. 等待对方的释放连接响应

6.5.4　同步练习参考答案

B

6.6　域名和地址

6.6.1　考点辅导

6.6.1.1　域名系统

域表示一个区域或者范围。域内可以容纳许多主机，因此并非每一台接入因特网的主机都必须具有一个域名地址，但是每一台主机都必须属于某个域，即通过该域的服务器可以查询和访问到这台主机。通常，该域服务器称为域名服务器(DNS)。对应因特网的层次结构，域采用嵌套结构与之对应。域名地址由一系列“子域名”组成，子域名的个数通常不超过5个，并且子域名之间用句点“.”分隔，从左到右子域的级别升高，高一级的子域包

含低一级的子域。这种嵌套的域名结构形成一棵域名树，树中的子节点和树叶标识分别表示不同的域，树叶被其上级的子节点或者树根所包含。这种域名结构也十分类似常用的通信地址(仅和我国表示地址的顺序有所不同)，符合人类表达的习惯。

因特网域名的取值遵守一定的规则。第一级域名通常分配给主干网节点，取值为国家名；第二级域名对应为次级节点，通常表示组网的部门或组织。二级域以下的域名由组网部门分配和管理。

6.6.1.2　地址分解协议

1. ARP 协议

ARP(Address Resolution Protocol)的功能是通过目标主机的 IP 地址，查询目标主机的 MAC 地址，实现了 IP 地址 MAC 地址的映射，保证通信的顺利进行。

ARP 协议使用一种询问/回答机制。如果主机 H1 要发送一个 IP 数据报给主机 H4，但它只知道 H4 的 IP 地址 P4，而不知道它的 MAC 地址。则按照图 6-4 所示的过程发送数据报。

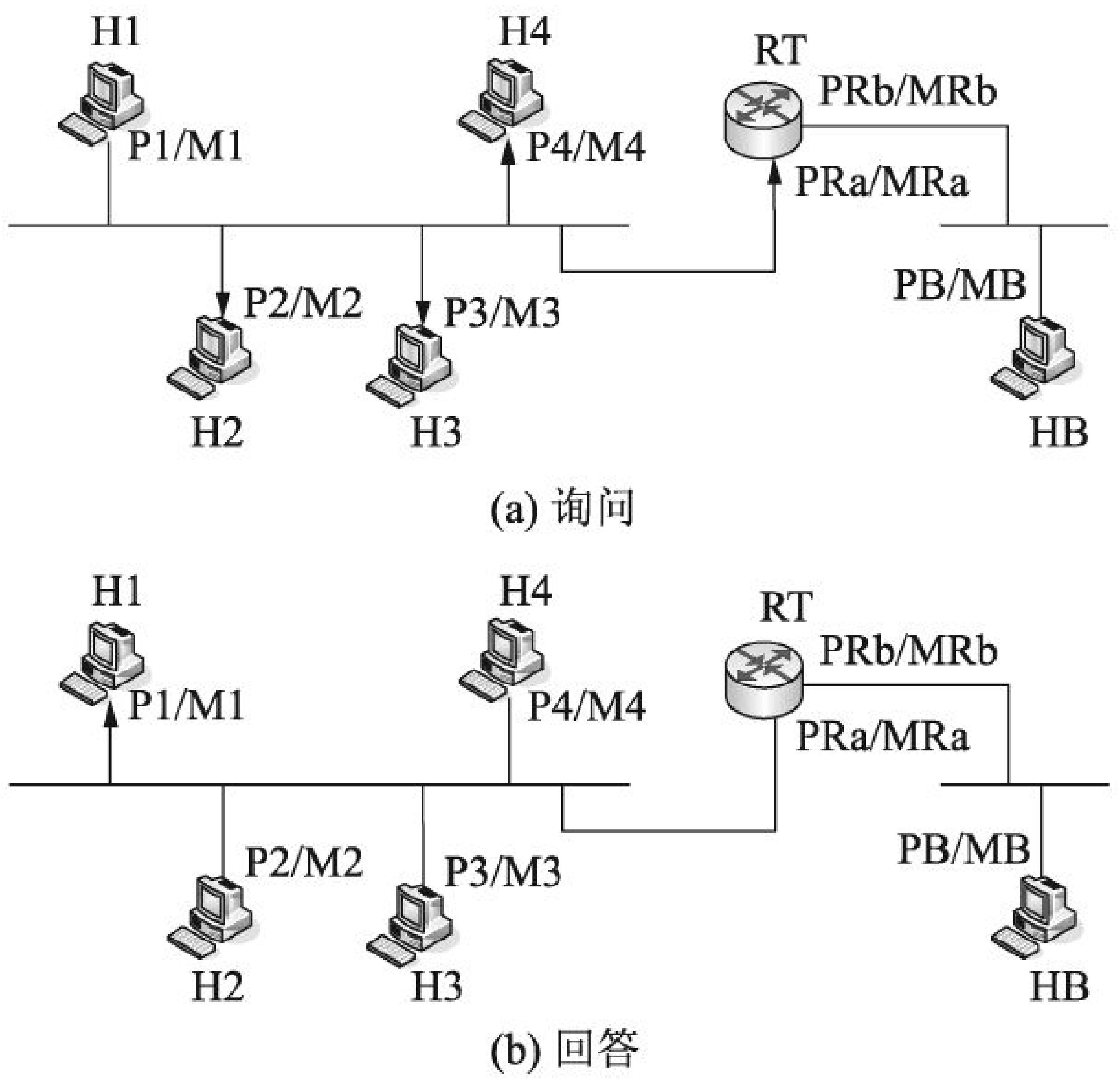


图 6-4　TCP 连接建立与释放

(1) H1 构造好 IP 数据报后，由于它不知道发放哪个 MAC 地址，还不能将其交给网卡处理。这时 H1 先构造一个 ARP 请求数据报，该数据报中包含了 H4 的 IP 地址 P4，并留下一个空位表示 H4 的 MAC 地址。H1 的 ARP 将该数据报交给网卡，让它将该数据报作为广播帧发送出去。

(2) 网络中的所有网卡收到该广播帧后将帧中的数据取出交给上层 ARP 处理。

(3) ARP 协议在收到这个请求数据报后将自己的 IP 地址与数据报中的 IP 地址进行比较，如果相同就表示对方在询问自己的 MAC 地址。如果发现不是询问自己的 MAC 地址，ARP 协议会丢弃该数据报。

(4) 只有 H4 会处理这个 ARP 请求数据报。这时 H4 将自己的 MAC 地址填在 MAC 地

址空位上，并将该数据报改为 ARP 响应数据报。由于 H1 在发送的请求数据报中填写了自己的 MAC 地址和 IP 地址，因此 H4 让网卡将 ARP 响应数据报以单播方式发送给主机 H1。

对于不在同一以太网的通信，该过程略有不同。例如，H1 要与 HB 通信，H1 知道自己与 HB 不在同一网络中，需要通过路由器将数据报发送给 HB，因此 H1 将 IP 数据报发送给路由器 RT。RT 将数据报转发给 HB 时，如果它不知道 HB 的 MAC 地址，它也会使用 ARP 进行询问。

如果每次发送一个 IP 数据报都需要进行一次 ARP 请求数据报的广播，那么发送一个 IP 数据报的代价是很高的。因此，通常在系统中维持一个 ARP 缓存，来减少地址解析所需的通信。

2. RARP 协议

RARP(Reverse Address Resolution Protocol，反向地址解析协议)的作用是将 MAC 地址转换为 IP 地址。某些主机(通常是无盘工作站)只知道自己的 MAC 地址，但有时候需要知道其 IP 地址，这就需要 RARP。为了使 RARP 正常工作，在局域网中至少有一台主机充当 RARP 服务器，并且要在 RARP 服务器中建立好 MAC 地址与 IP 地址的映射表。

6.6.2 典型例题分析

例 6-28 某客户机请求 Web 站点服务的以太网数据帧(前 160 字节)如下图所示，则客户机默认网关的物理地址为__(28)__。客户机在查找默认网关的物理地址时使用的协议是__(29)__，发出的数据帧中目的 MAC 地址为__(30)__。(2017 年上半年真题 28、29、30)

```
0000   00 23 89 1a 06 7c 00 1d   7d 39 62 3e 08 00 45 00   ......|..     }9b>//E.
0010   01 3b 36 43 40 00 40 06   17 d1 db f5 43 de 7b 7d   .;6C0.0.      ....c.{}
0020   50 58 06 55 00 50 34 94   05 db b7 cf 20 28 50 18   PX.U.P4       ....(P.
0030   ff ff ec d6 00 00 47 45   54 20 2f 71 2e 68 74 6d   ......GE      T /q.htm
0040   6c 3f 6e 61 6d 65 3d 45   78 74 53 6d 61 72 74 77   1?name=E      xtSmartw
0050   69 7a 49 45 26 73 65 76   65 72 3d 36 2e 30 2e 32   izIE&sev      er=6.0.2
0060   39 30 30 2e 32 31 38 30   26 61 70 70 76 65 72 3d   900.2180      &appver=
0070   31 2e 30 2e 30 2e 31 30   30 37 26 6d 69 64 3d 64   1.0.0.10      07&mid=d
0080   30 38 63 37 39 33 30 34   35 36 63 61 30 66 34 61   08c79304      56ca0f4a
0090   34 39 33 32 36 33 63 32   37 36 35 62 37 34 32 26   493263c2      765b742&
```

(28) A. 00-23-89-1a-06-7c　　B. 00-ld-7d-39-62-3e
　　C. 00-00-00-00-00-00　　D. ff-ff-ff-ff-ff

(29) A. FTP　　B. ARP　　C. BGP　　D. ICMP

(30) A. 00-23-89-1a-06-7c　　B. 00-ld-7d-39-62-3e
　　C. 00-00-00-00-00-00　　D. ff-ff-ff-ff-ff

解析：默认网关参考第一条记录，后面的是网关的物理地址。ARP 的功能是通过目标主机的 IP 地址，查询目标之间的 MAC 地址，实现 IP 地址与 MAC 地址的映射，从而保证通信的顺利进行。

答案：(28) A　(29) B　(30) D

例 6-29　下面哪个协议可通过主机的逻辑地址查找对应的物理地址？__(20)__(2016 年下半年真题 20)

A. DHCP　　B. SMTP　　C. SNMP　　D. ARP

解析：ARP 的功能是通过目标主机的 IP 地址，查询目标主机的 MAC 地址，实现了 IP 地址与 MAC 地址的映射，保证通信的顺利进行。

答案：D

例 6-30　代理 ARP 是指__(22)__。(2016 年下半年真题 22)

A. 由邻居交换机把 ARP 请求传送给远端目标

B. 由一个路由器代替远端目标回答 ARP 请求

C. 由 DNS 服务器代替远端目标回答 ARP 请求

D. 由 DHCP 服务器分配一个回答 ARP 请求的路由器

解析：路由器从开启 ARP 代理的接口收到一个 ARP 请求，该目标 IP 地址是可达的，而且这个对应的路由条目的接口不是收到该 ARP 请求的接口，那么路由器将执行代理 ARP 功能。

答案：B

例 6-31　在进行域名解析过程中，当主域名服务器查找不到 IP 地址时，由__(34)__负责域名解析。(2016 年下半年真题 34)

A. 本地缓存　　B. 辅助域名服务器

C. 根域名服务器　　D. 转发域名服务器

解析：主域名服务器：负责维护一个区域的所有域名信息，是特定的所有信息的权威信息源，数据可以修改。

辅助域名服务器：当主域名服务器出现故障、关闭或负载过重时，辅助域名服务器作为主域名服务器的备份提供域名解析服务。辅助域名服务器中的区域文件中的数据是从另外的一台主域名服务器中复制过来的，是不可以修改的。

缓存域名服务器：从某个远程服务器取得每次域名服务器的查询回答，一旦取得一个回答就将它放在高速缓存中，以后查询相同的信息就用高速缓存中的数据回答。缓存域名服务器不是权威的域名服务器，因为它提供的信息都是间接信息。

转发域名服务器：负责所有非本地域名的本地查询。转发域名服务器接到查询请求后，在其缓存中查找，如找不到就将请求依次转发到指定的域名服务器，直到查找到结果为止，否则返回无法映射的结果。

根域名服务器：根域名服务器知道所有顶级域名服务器的域名和 IP 地址，只要本地域名无法解析，都首先求助于根域名服务器。

答案：C

例 6-32　DNS 反向搜索功能的作用是__(32)__，资源记录 MX 的作用是__(33)__，DNS 资源记录__(34)__定义了区域的反向搜索。(2016 年上半年真题 32～34)

(32)、(33) A. 定义域名服务器的别名　　B. 将 IP 地址解析为域名

C. 定义域邮件服务器的地址和优先级　　D. 定义区域的授权服务器

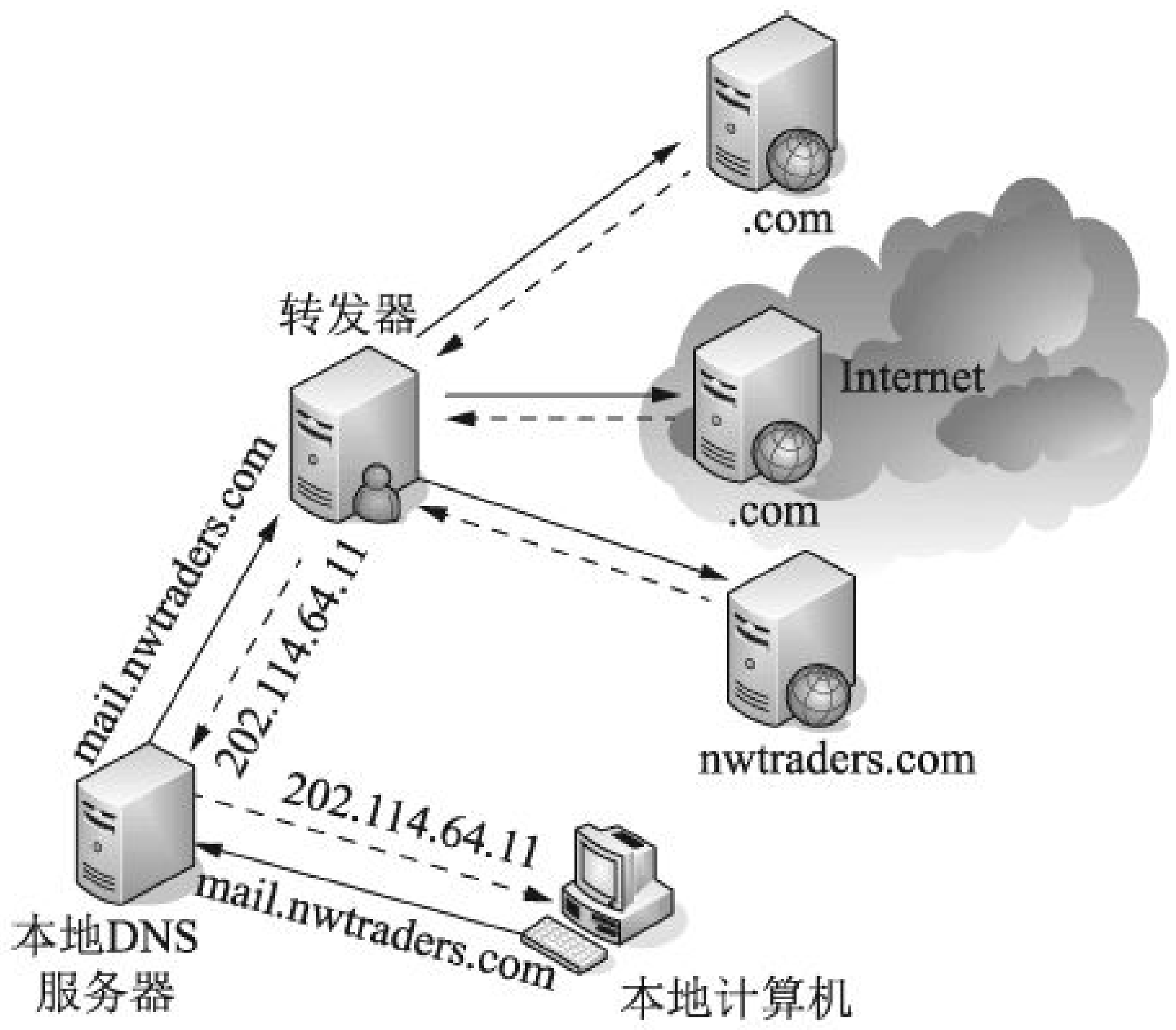
(34) A. SOA　　B. NS　　C. PTR　　D. MX

解析：DNS 正向搜索功能的作用是将域名解析为 IP 地址，反向搜索功能的作用是将 IP 地址解析为域名。资源记录 MX 的作用是定义域邮件服务器地址和优先级。

定义了区域的反向搜索的是 DNS 资源记录 PTR。

答案：(32) B (33) C (34) C

例 6-33 下图是 DNS 转发器工作的过程。采用迭代查询算法的是___(35)___。(2015 年下半年真题 35)



A. 转发器和本地 DNS 服务器　　B. 根域名服务器和本地 DNS 服务器

C. 本地 DNS 服务器和.com 域名服务器　　D. 根域名服务器和.com 域名服务器

解析：只要发出递归查询，服务器必须回答目标 IP 与域名的映射关系。而迭代查询是，服务器收到一次迭代查询，回复一次结果，这个结果不一定是目标 IP 与域名的映射关系，也可以是其他 DNS 服务器的地址。

一般情况下从客户端到本地 DNS 服务器是属于递归查询，而 DNS 服务器之间的交互查询就是迭代查询。

答案：D

例 6-34 下列域名中，格式正确的是___(36)___。(2015 年下半年真题 36)

A. -123456.com　　B. 123-456.com

C. 123*456.com　　D. 123456-.com

解析：本题目考查域名的基础知识。

一个合法的域名可以由字母、数字、下画线构成，不能存在除以上三种字符之外的其他字符，并且不能以下画线开始和结束。

答案：B

例 6-35 以下关于域名查询的叙述中，正确的是___(37)___。(2015 年下半年真题 37)

A. 正向查询是检查 A 记录，将 IP 地址解析为主机名

B. 正向查询是检查 PTR 记录，将主机名解析为 IP 地址

C. 反向查询是检查 A 记录，将主机名解析为 IP 地址

D. 反向查询是检查 PTR 记录，将 IP 地址解析为主机名

解析：DNS 资源记录如下。

SOA 记录：SOA 说明能解析这个区域的 DNS 服务器中哪个是主服务器。

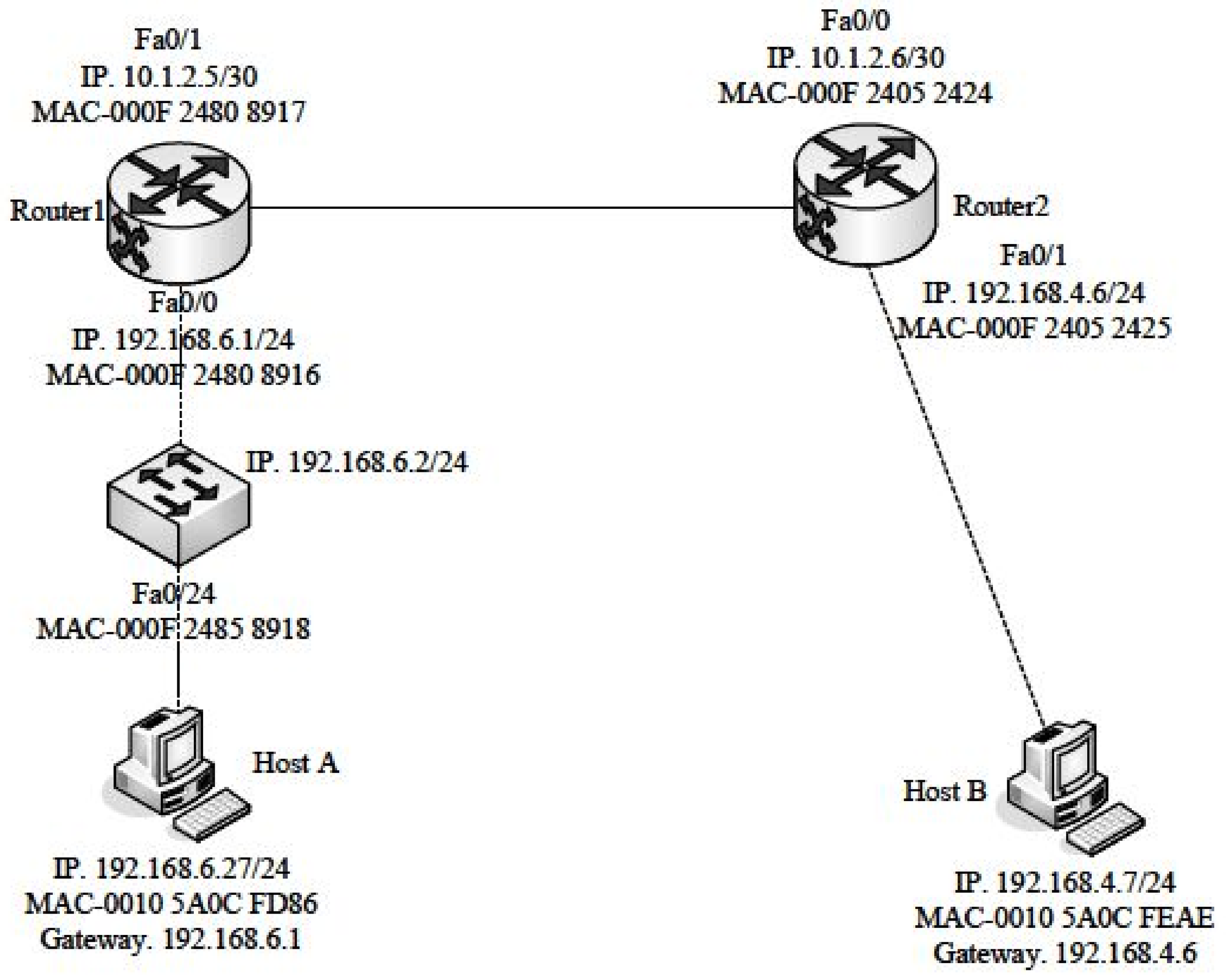
NS 记录：用于标识区域的 DNS 服务器有几台提供服务。

A 记录：也称为主机记录，是 DNS 名称到 IP 地址的映射，用于正向解析。

PTR 记录：IP 地址到 DNS 名称的映射，用于反向解析。

答案：D

例 6-36　参见下面的网络连接图，4 个选项是 Host A 的 ARP 表，如果 Host A ping HostB，则 ARP 表中的哪一选项用来封装传输的帧？<u>(61)</u> (2015 年上半年真题 61)



	Interface Address	Physical Address	Type
A.	192.168.4.7	000f 2480 8916	dynamic
B.	192.168.4.7	0010 5a0c feae	dynamic
C.	192.168.6.2	0010 5a0c feae	dynamic
D.	192.168.6.1	000f 2480 8916	dynamic

解析：主机如果需要发送数据到与自身不同网段的地址时，它会将数据包发给网关，靠网关来帮它转发。一开始的时候，主机是通过 ARP 来寻找网关的 MAC 地址的，获得网关的 MAC 地址后，主机就可以直接把数据包发给网关了。

答案：D

6.6.3　同步练习

在进行域名解析过程中，由______获取的解析结果耗时最短。

A. 主域名服务器　　　B. 辅助域名服务器

C. 缓存域名服务器　　　D. 转发域名服务器

6.6.4　同步练习参考答案

C

6.7　网 关 协 议

6.7.1　考点辅导

Internet 中的路由器称为 IP 网关。网关协议用于网关之间交换路由信息。

1. 自治系统

自治系统是由同构型的网关连接的互联网，这样的系统往往是由一个网络管理中心控

制的。自治系统内部的网关之间执行内部网关协议(IGP)，互相交换路由信息。IGP 是自治系统内部专用的，为特定的应用服务，在自治系统之外是无效的。

一个互联网也可能由不同的自治系统互联而成。在这种情况下，不同的自治系统可能采用不同的路由表和不同的路由选择算法。在不同自治系统中的网关之间交换路由信息，要用外部网关协议(EGP)。EGP 比 IGP 传送的信息要少一些，因为 EGP 只涉及自治系统之间的路由信息，而与系统内部路由无关。EGP 以自治系统为节点，通告各个网关可到达哪些系统。

2. 外部网关协议

自治系统之间使用 EGP，最新的 EGP 叫作边界网关协议(BGP)。BGP 的主要功能是控制路由策略，如是否愿意转发过路的分组等。BGP 的报文通过 TCP 连接传送。BGP 报文可实现以下 3 个功能过程。

(1) 建立邻居关系。位于不同自治系统中的两个路由器首先要建立邻居关系，然后才能周期性地交换路由信息。建立邻居关系的过程是：一个路由器发送 open 报文，另一个路由器若愿意接受请求，则以 keepalive(保持活动状态)报文应答。

(2) 邻居可达性。这个过程维护邻居关系的有效性。通过周期性地互相发送 keepalive 报文，双方都知道对方的活动状态。

(3) 网络可达性。每个路由器保持一个数据库，记录着它可到达的所有子网。当情况有变化时，用更新报文把最新信息及时地广播给所有实现 BGP 的路由器。

3. 内部网关协议

Internet 的内部路由协议经过了几次大的变化。最初的 RIP(路由选择信息协议)是基于 Bellman-Ford 算法的延迟矢量协议。这个协议在网络规模不大时工作得较好，当网络规模扩大后，因为交换的路由信息太多而显得效率很低。于是，在 1979 年 5 月被另一个路由协议——基于 Dijkstra 算法的链路状态协议所取代。从 1988 年开始，IETF 开始研制新的路由协议，这就是 OSPF(开放最短路径优先)协议。1990 年，OSPF 正式成为新的内部路由协议标准。

OSPF 基本上仍是一种链路状态协议。OSPF 的路由器维护一个本地链路状态表，并随时向其他相邻的路由器发送关于链路状态的更新信息。通过周期地扩散传播链路状态信息，每个路由器都记住了关于网络拓扑结构的全局数据库。同时 OSPF 路由器根据用户指定的链路费用标准(延迟、带宽或收费率等)计算最短通路，由到达各个目标的最短通路构成路由表。OSPF 报文包含在原始的 IP 数据报中传送。

4. 核心网关协议

Internet 中有一个主干网，所有的自治系统都连接到主干网上。主干网中的网关叫核心网关。核心网关之间交换路由信息时使用网关到网关协议(GGP)。这里需要区分 EGP 和 GGP：EGP 用于两个不同自治系统中的网关之间交换路由信息；而 GGP 是主干网中的网关协议。因为主干网中的核心网关是由 InterNOC(网络操作中心)直接控制的，所以 GGP 更具有专用性。当一个核心网关加入主干网时用 GGP 协议向邻机广播发送它所连接的网络的路由信息，各邻机更新路由表，并进一步传播新的路由信息。

GGP 协议的报文分为 4 类。

- 路由更新报文：发送路由信息。
- 应答报文：对路由更新报文的应答，分肯定/否定两种。
- 测试报文：测试相邻网关是否存在。
- 网络接口状态报文：测试本地网络连接的状态。

6.7.2　典型例题分析

例 6-37　以下关于 OSPF 路由协议的描述中，错误的是__(19)__。(2017 年下半年真题 19)

A. 采用 Dijkstra 算法计算到达各个目标的最短通路

B. 计算并得出整个网络的拓扑视图

C. 向整个网络中每一个路由器发送链路代价信息

D. 定期向邻居发送 keepalive 报文表明存在

解析：OSPF 基本上仍是一种链路状态协议。OSPF 的路由器维护一个本地链路状态表，并随时向其他邻居的路由发送关于链路状态的更新信息，并不是向网络中每一个路由器发送链路代价信息。

答案：C

例 6-38　在 BGP4 协议中，当接收到对方 open 报文后，路由器采用__(28)__报文响应，从而建立两个路由器之间的邻居关系。(2017 年下半年真题 28)

A.hello　　B.update　　C.keepalive　　D. notification

解析：BGP 中，接收到对方 open 报文后，若有错则发出 notification。若能建立连接，则发出 keepalive，用来确认 open 报文和周期性地证实邻居关系。

答案：C

例 6-39　OSPF 协议把网络划分成 4 种区域(Area)，其中__(27)__不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。(2017 年上半年真题 27)

A. 分支区域　　B. 标准区域　　C. 主干区域　　D. 存根区域

解析：如果将区域看成一个节点，则 OSPF 是以主干区域(ared0)为顶点，其他区域为终端的星型拓扑结构。

标准区域可以接收链路更新信息和路由总结。

存根区域是不接收自治系统以外的路由信息的区域。如果需要自治系统以外的路由，它使用默认路由 0.0.0.0。

答案：D

例 6-40　RIPv2 对 RIPvl 协议的改进之一为：路由器有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源，这种方案称为__(25)__，其作用是__(26)__。(2017 年上半年真题 25、26)

(25) A. 反向毒化　　B. 乒乓反弹　　C. 水平分割法　　D. 垂直划分法

(26) A. 支持 CIDR　　B. 解决路由环路

C. 扩大最大跳步数　　D. 不使用广播方式更新报文

解析：水平分割法，从一个方向来的路由信息，不能再放入发回那个方向的路由更新

包并又发回那个方向。这是一种能解决路由环路的有效方法。

答案：(25) C　(26) B

例 6-41　如果路由器收到了多个路由协议转发的、关于某个目标的多条路由，它如何决定采用哪个路由？__(23)__(2016 年下半年真题 23)

A. 选择与自己路由协议相同的　　B. 选择路由费用最小的

C. 比较各个路由的管理距离　　D. 比较各个路由协议的版本

解析：各种路由来源的管理距离如下表所示。

路由来源	管理距离	路由来源	管理距离
直连路由	0	IS-IS	115
静态路由	1	RIP	120
EIGRP 汇总路由	5	EGP	140
外部 BGP	20	ODR(按需路由)	160
内部 EIGRP	90	外部 EIGRP	170
IGRP	100	内部 BGP	200
OSPF	110	未知	255

如果路由器收到了由多个路由协议转发的、关于某个目标的多条路由，则比较各个路由的管理距离，并采用管理距离小的路由来源提供的路由信息。

答案：C

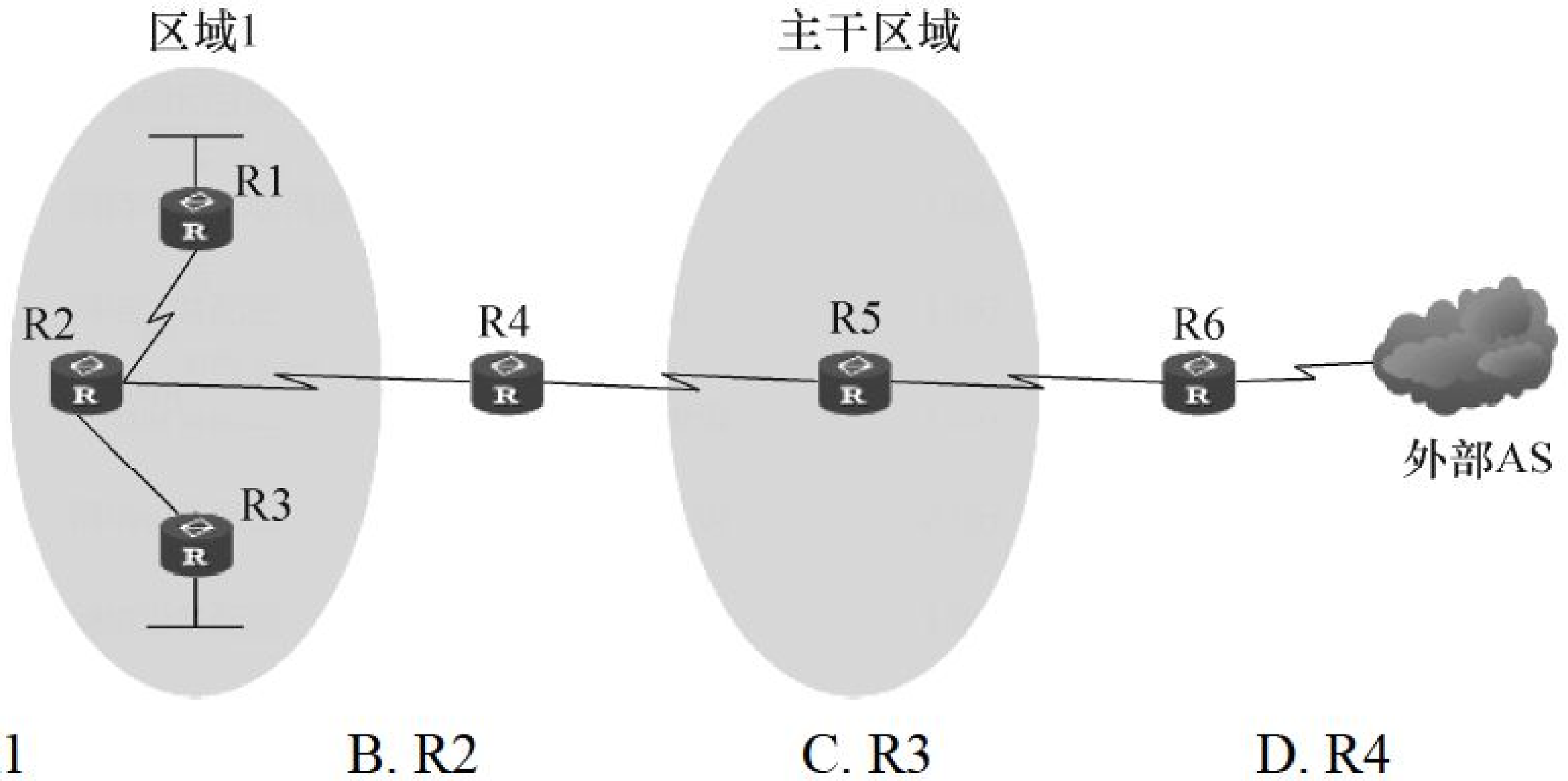
例 6-42　下面的选项中属于链路路由选择协议的是__(24)__。(2016 年下半年真题 24)

A. OSPF　　B. IGRP　　C. BGP　　D. RIPv2

解析：IGRP、BGP、RIPv2 是距离矢量路由协议。运行链路状态路由协议的路由器，在相互学习路由之间，会首先向自己的邻居路由学习整个网络的拓扑结构，并在自己的内存中建立一个拓扑表，然后使用最短路径优先(SPF)算法，从自己的拓扑表中计算出路由来。OSPF 协议就是一个典型的链路路由选择协议。

答案：A

例 6-43　下面的 OSPF 网络由多个区域组成。在这些路由器中，属于主干路由器的是__(25)__，属于自治系统边界路由器(ASBR)的是__(26)__。(2016 年下半年真题 25、26)



(25) A. R1　　B. R2　　C. R3　　D. R4

(26) A. R3　　B. R4　　C. R5　　D. R6

解析：主干路由器是指至少有一个接口定义为主干区域的路由器。任何一个和主干区域互联的 ABR 或者 ASBR 也将称为主干路由器。AS 边界路由器是和 AS 外部的路由器互相交换路由信息的 OSPF 路由器。该路由器在 AS 内部通告其所得到的 AS 外部路由信息，这样的话，AS 内部的所有的路由器都能够知道 AS 边界路由器的路由信息。

答案：(25) D　(26) D

例 6-44　RIPv2 与 RIPv1 相比，它改进了什么？__(27)__(2016 年下半年真题 27)

A. RIPv2 的最大跳数扩大了，可以适应规模更大的网络

B. RIPv2 变成无类别的协议，必须配置子网掩码

C. RIPv2 用跳数和带宽作为度量值，可以有更多的选择

D. RIPv2 可以周期性地发送路由更新，收敛速度比原来的 RIP 快

解析：RIPv1 和 RIPv2 版本的区别是：RIPv1 是有类别的路由协议，它只支持以广播方式发布协议报文。RIPv1 的协议报文无法携带掩码信息，它只能识别 A、B、C 类标准分类网段的路由，而 RIPv2 是一种无类别路由协议，使用 224.0.0.9 的组播地址，支持 MD5 认证。

答案：B

例 6-45　为了解决伴随 RIP 协议的路由环路问题，可以采用水平分割法，这种方法的核心是__(22)__，而反向毒化方法则是__(23)__。(2016 年上半年真题 22、23)

(22)、(23)　A. 把网络水平地分割为多个网段，网段之间通过指定路由器发布路由信息
B. 一条路由信息不要发送给该信息的来源
C. 把从邻居学习到的路由费用设置为无限大并立即发送给那个邻居
D. 出现路由变化时立即向邻居发送路由更新报文

解析：水平分割法的规则和原理是：路由器从某个接口接收到的更新信息不允许再从这个接口发回去。此方法不仅能够阻止路由环路的产生，还能减少路由器更新信息占用的链路带宽资源。反向毒化即保证所有的邻居路由被毒化，会向“毒源”的方向反向“毒化”。

答案：(22) B　(23) C

例 6-46　OSPF 网络被划分为各种区域，其中作为区域之间交换路由信息的是__(24)__。(2016 年上半年真题 24)

A. 主干区域　　B. 标准区域　　C. 存根区域　　D. 不完全存根区域

解析：为了使 OSPF 能用于规模很大的网络，OSPF 将一个自治系统再划分为若干个更小的范围，叫作区域。为了使每一个区域能够和本区域以外的区域进行通信，OSPF 使用层次结构的区域划分，在上层的区域叫作主干区域，主干区域的标识符为 0.0.0.0，其作用是连通其他在下层的区域，从其他区域来的信息都由区域边界路由器进行概括。

答案：A

例 6-47　OSPF 将路由器连接的物理网络划分为以下 4 种类型，以太网属于__(25)__，X.25 分组交换网属于__(26)__。(2016 年上半年真题 25、26)

(25)、(26)　A. 点到点网络　　B. 广播多址网络
C. 点到多点网络　　D. 非广播多址网络

解析：根据路由器所连接的物理网络不同，OSPF 将网络划分为 4 种类型：广播多路访问(Broadcast multiAccess)型、非广播多路访问(None Broadcast multiAccess)型、点到点(Point-to-Point)型、点到多点(Point-to-MultiPoint)型。其中：广播多路访问型网络如 Ethernet、

Token Ring、FDDI，非广播多路访问型网络如 Frame Relay.X.25、SMD5，点到点型网络如 PPP、HDLC。

答案：(25) B (26) D

例 6-48 边界网关协议 BGP4 是一种动态路由发现协议，它的主要功能是__(24)__。BGP 路由器之间传送的是 AS 路径信息，这样就解决了__(25)__问题。BGP4 报文封装在__(26)__中。(2015 年下半年真题 24～26)

(24) A. 发现新的路由　　B. 计算最短通路
C. 控制路由策略　　D. 维护网络拓扑数据库

(25) A. 路由环路　　B. 最短通路
C. 路由计算　　D. 路由更新

(26) A. IP 数据报　　B. 以太帧
C. TCP 报文　　D. UDP 报文

解析：边界网关协议(BGP)是运行于 TCP 上的一种自治系统的路由协议。BGP 的主要目标是为处于不同 AS 中的路由器之间进行路由信息通信提供保障，只是力求寻找一条能够到达目的网络且比较好的路由，而不是要寻找一条最佳路由。BGP 既不是纯粹的矢量距离协议，也不是纯粹的链路状态协议，通常被称为通路向量路由协议。这是因为 BGP 在发布到一个目的网络的可达性的同时，包含了在 IP 分组到达目的网络过程中所必须经过的 AS 的列表。BGP 系统的主要功能是交换其他 BGP 系统的网络可达信息，包括 AS 路径的列表信息，此信息可用于建立 AS 系统连接图，以消除路由环路，及执行 AS 策略的确定。

答案：(24) C (25) A (26) C

例 6-49 在广播网络中，OSPF 协议要选定一个指定路由器(DR)，指定路由器的功能是__(27)__。(2015 年下半年真题 27)

A. 发送链路状态公告　　B. 检查网络故障
C. 向其他路由器发送最新路由表　　D. 发现新增加的路由

解析：为减少网络中的链路状态公告(也称通告)(LSA)分组泛洪传播，OSPF 协议会在每一个网络中选举一个指定路由器(DR)和一个备用指定路由器(BDR)。网络中的路由器都只与 DR、BDR 建立全相邻的邻接关系，其他路由器之间不会建立全相邻的 OSPF 邻接关系。在 OSPF 网络中，各路由器之间不直接两两发链路状态信息，而是通过选举 DR/BDR，DR 为主，BDR 为备份 DR，把链路状态信息发给 DR/BDR，由 DR 再组播给所有非 DR/BDR 的路由器。

答案：A

例 6-50 以下关于 OSPF 的区域(Area)的叙述中，正确的是__(17)__。(2015 年上半年真题 17)

A. 各个 OSPF 区域都要连接到主干区域　　B. 分层的 OSPF 网络不需要多个区域
C. 单个 OSPF 网络只有区域 1　　D. 区域 ID 的取值范围是 1～32 768

解析：区域 ID 长 32 位，其表示范围为 0～65 535。当设置 area 0 时，其区域 ID 为 0.0.0.0。当网络区域为 0 或 0.0.0.0 时称为主干区域。作为主干区域的 area 0 必须存在；所有区域，即使是端区，也必须和骨干区域相连；如果存在多个骨干区域，那么它们必须连续(逻辑上)。

答案：A

例 6-51 运行 OSPF 协议的路由器用__(18)__报文来建立和更新它的拓扑数据库。(2015

年上半年真题 18)

A. 由其他路由器发送的链路状态公告(LSA)

B. 从点对点链路收到的信标

C. 由指定路由器收到的 TTL 分组

D. 从邻居路由器收到的路由表

解析：链路状态公告(LSA)就是 OSPF 接口上的描述信息，例如接口上的 IP 地址、子网掩码、网络类型、Cost 值等。OSPF 路由器之间交换的并不是路由表，而是链路状态公告(LSA)。OSPF 通过获得网络中所有的链路状态信息，从而计算出到达每个目标的精确的网络路径。OSPF 路由器会将自己所有的链路状态信息毫不保留地全部发给邻居，邻居将收到的链路状态信息全部放入链路状态数据库(Link-State Database)；邻居再发给自己的所有邻居，并且在传递过程中，绝对不会有任何更改。通过这样的过程，最终，网络中所有的 OSPF 路由器都拥有网络中所有的链路状态信息，并且所有路由器的链路状态信息应该能描绘出相同的网络拓扑。

答案：A

例 6-52　链路状态路由协议的主要特点是__(19)__。(2015 年上半年真题 19)

A. 邻居之间交换路由表　　　　B. 通过事件触发及时更新路由

C. 周期性更新全部路由表　　　D. 无法显示整个网络拓扑结构

解析：链路状态路由协议只在网络发生变化的时候发送触发式更新(triggered update)，更新是非周期性的。

答案：B

6.7.3　同步练习

1.　边界网关协议 BGP4 被称为路径矢量协议，它传送的路由信息是由一个地址前缀后跟__(1)__组成，这种协议的优点是__(2)__。

(1) A. 一串 IP 地址　　　　B. 一串自治系统编号

C. 一串路由器编号　　　D. 一串子网地址

(2) A. 防止域间路由循环　　B. 可以及时更新路由

C. 便于发现最短通路　　D. 考虑了多种路由度量因素

2.　与 RIPv2 相比，IGRP 协议增加了一些新的特性，下面的描述中错误的是______。

A. 路由度量不再把跳步数作为唯一因素，还包含了带宽、延迟等参数

B. 增加触发更新来加快路由收敛，不必等待更新周期结束再发送更新报文

C. 不但支持相等费用负载均衡，而且支持不等费用的负载均衡

D. 最大跳步数由 15 跳扩大到 255 跳，可以支持更大的网络

3.　为了解决 RIP 协议形成路由环路的问题可以采用多种方法，下面列出的方法中效果最好的是__(25)__。

A. 不要把从一个邻居学习到的路由发送给那个邻居

B. 经常检查邻居路由器的状态，以便及时发现断开的链路

C. 把从邻居学习到的路由设置为无限大，然后再发送给那个邻居

D. 缩短路由更新周期，以便出现链路失效时尽快达到路由无限大

4. OSPF 协议将其管理的网络划分为不同类型的若干区域(Area)，其中标准区域的特点是__(1)__，存根区域(stub)的特点是__(2)__。

(1)、(2)A. 不接收本地 AS 之外的路由信息，也不接收其他区域的路由汇总信息

B. 不接收本地 AS 之外的路由信息，对本地 AS 之外的目标采用默认路由

C. 可以接收任何链路更新信息和路由汇总信息

D. 可以学习其他 AS 的路由信息，对本地 AS 中的其他区域采用默认路由

6.7.4 同步练习参考答案

1. (1) B (2) A 2. B 3.A 4. (1) C (2) B

6.8 路由技术

6.8.1 考点辅导

6.8.1.1 NAT 技术

NAT 技术主要解决 IP 地址短缺的问题。最初提出的建议是在子网内部使用局部地址，而在子网外部使用少量的全局地址，通过路由器进行内部地址和外部地址的转换。局部地址是在子网内部独立编址的，可以与外部地址重叠。这种想法的基础是假定在任何时候子网中只有少数计算机需要与外部通信，可以让这些计算机共享少量的全局 IP 地址。后来根据这种技术又开发出其他一些应用，如动态地址翻译、伪装等。

(1) 动态地址翻译的好处是节约了全局 IP 地址，而且不需要改变子网内部的任何配置，只需在边界路由器中设置一个动态地址变换表就可以工作了。

(2) 伪装技术使用一个路由器的 IP 地址就可以把子网中所有主机的 IP 地址都隐藏起来。

6.8.1.2 CIDR 技术

1. 无分类域间路由选择(CIDR)

无分类域间路由选择(CIDR)消除了传统 A 类、B 类和 C 类地址以及划分子网的概念，从而可以更加有效地分配 IPv4 的地址空间。CIDR 使用各种长度的“网络前缀”(Network-Prefix)来代替分类地址中的网络号和子网号，而不像分类地址中只使用 1 字节、2 字节和 3 字节长的网络号。CIDR 不再使用“子网”概念而使用网络前缀，使 IP 地址从三级编址(使用子网掩码)又回到两级编址，但这是一个无分类的两级编址。CIDR 使用“斜线记法”，它又称为 CIDR 记法，即在 IP 地址后面加上一斜线“/”，然后写上网络前缀所占的比特数(这个数值对应于三级编址中子网掩码中比特 1 的个数)。例如，128.14.146.158/20，表示在这 32 比特中，前 20 比特表示网络前缀，后面 2 比特为主机号。

CIDR 将网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”。一个 CIDR 地址块是由地址块的起始地址(即地址块中地址块数值最小的一个)和地址块中的地址数来定义的。CIDR 地址块也可用斜线记法来表示。例如，128.14.32.0/20 表示的地址块共有 2^{12} 个地址，这个地址的起始地址是 128.14.32.0。

2. 超网

超网技术是将几个小的网络组成一个大的网络。例如，一个组织需要 1000 个地址，申请 4 个 C 类地址，可以把 4 个 C 类地址合并为一个超网，如图 6-5 所示。CIDR 技术实现了超网。

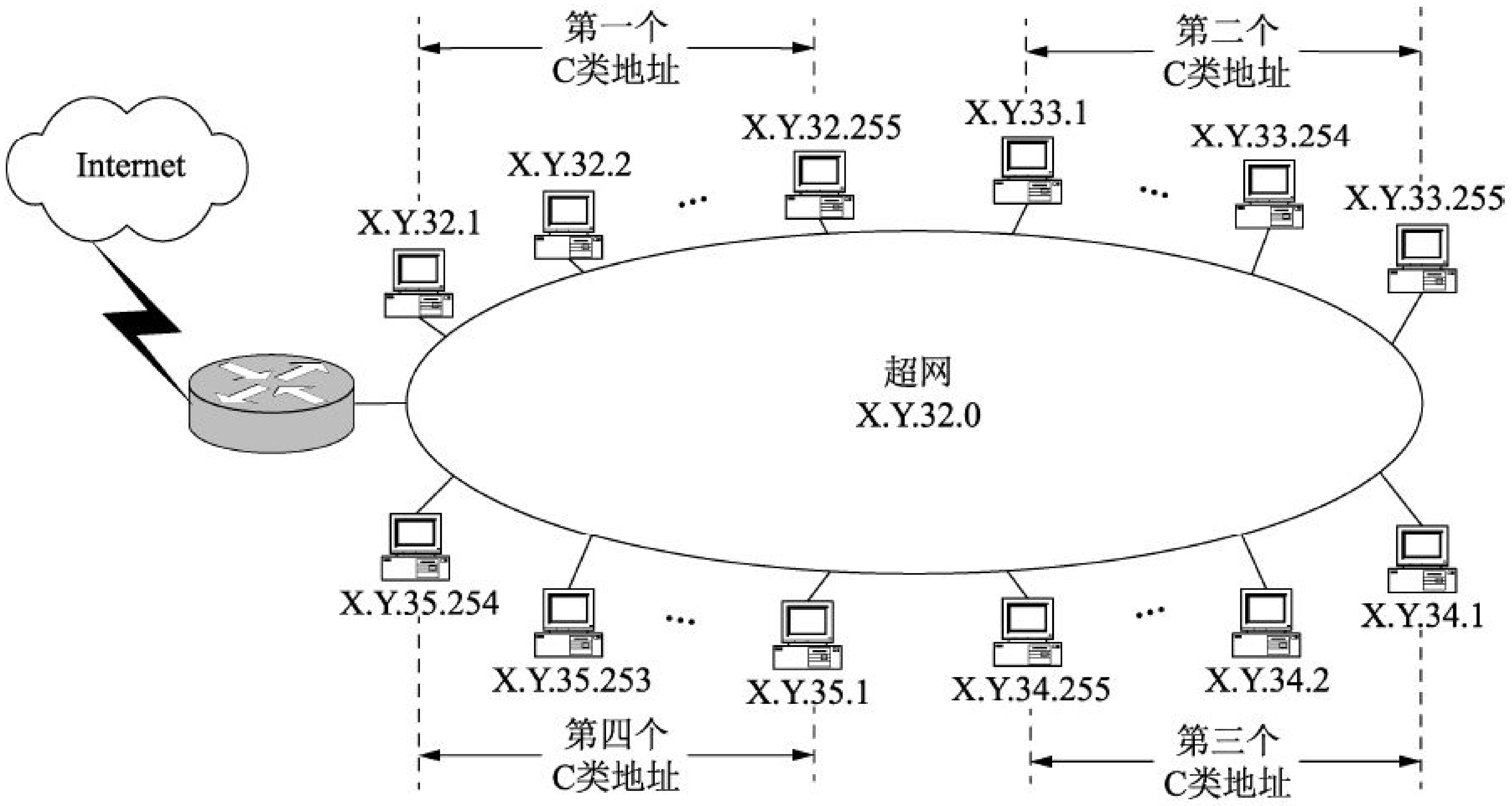


图 6-5　超网

3. 路由汇总

路由汇总也称路由聚合，其实现方法与超网相同，但它的主要目的是减少路由表的网络数目，减轻路由器的负担。在大型的网络中，可能包含几十万条 IP 路由，有些存储容量较小的路由器无法容纳如此庞大的路由信息，使用路由汇总可以合并几个网络地址为一个代表这几个网络的聚合网络地址。

设有下面 4 条路由：172.18.129.0/24、172.18.130.0/24、172.18.132.0/24 和 172.18.133.0/24，进行路由汇聚，能覆盖这 4 条路由的地址是 172.18.128.0/21。计算方法是找出 4 条路由的网络地址的共同前缀和位数，计算过程如图 6-6 所示。

172.18.129.0/24:		10101100	00010010	10000	001	00000000
172.18.130.0/24:		10101100	00010010	10000	010	00000000
172.18.132.0/24:		10101100	00010010	10000	100	00000000
172.18.133.0/24:		10101100	00010010	10000	101	00000000
相同位 21:		10101100	00010010	10000	000	00000000
		(172)	(18)	(128)		(0)

图 6-6　路由汇聚的过程

6.8.1.3 第三层交换技术

1. 3 层交换机

第三层交换技术是指利用第二层交换的高带宽和低延迟优势尽快地传送网络层分组的技术。交换和路由不同，前者用硬件实现，速度快，而后者由软件实现，速度慢。3 层交换机的工作原理可以概括为：一次路由，多次交换。也就是说，当 3 层交换机第一次收到一个数据包时必须通过路由功能寻址转发端口，同时记住目标 MAC 地址和源 MAC 地址，以及其他有关信息，当再次收到目标地址和源地址相同的帧就直接进行交换，不再调用路由功能。所以 3 层交换机不但具有路由功能，而且比通常的路由器转发得更快。

下面将通过一个简单的网络来看看 3 层交换机的工作过程。

假设有两台主机(分别是主机 A、主机 B)挂接在 3 层交换机上。比如，主机 A 要给主机 B 发送数据，则 3 层交换机的工作过程如下。

(1) 已知目的 IP，那么主机 A 就用其本身的子网掩码与该目的 IP 相与，取得目的网络号，判断目的 IP 是否与自己在同一网段。

(2) 如果在同一网段，但不知道转发数据所需的 MAC 地址，主机 A 就发送一个 ARP 请求，主机 B 返回其 MAC 地址；然后，主机 A 用此 MAC 封装数据包并发送给交换机，交换机启用 2 层交换模块，查找 MAC 地址表，将数据包转发到相应的端口。

(3) 如果目的 IP 地址不是同一网段的，那么主机 A 要实现和主机 B 的通信，主机 A 就将第一个正常数据包发送给一个默认网关。这个默认网关一般在操作系统中已经设好，对应第三层路由模块；所以对于不是同一子网的数据，最先在数据包中目的 MAC 地址中放入的是默认网关的 MAC 地址。然后由 3 层模块接收此数据包，查询路由表以确定到达主机 B 的路由。构造一个新的帧头，其中以默认网关的 MAC 地址为源 MAC 地址，以主机 B 的 MAC 地址为目的 MAC 地址。通过一定的识别触发机制，确立主机 A 与主机 B 的 MAC 地址及转发端口的对应关系，并记录进 3 层交换机流缓存条目表。以后的主机 A 到主机 B 的数据，就直接交由 2 层交换模块完成。这就是通常所说的一次路由，多次转发。

2. MPLS

IETF 开发的多协议标签交换(MultiProtocol Label Switching，MPLS，RFC3031)把第二层的链路状态信息(带宽、延迟、利用率等)集成到第三层的协议数据单元中，从而简化和改进了第三层分组的交换过程。理论上，MPLS 支持任何第二层和第三层协议。MPLS 报头的位置介于第二层和第三层之间，可称为第 2.5 层。MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包，甚至 ATM 信元等。

1) MPLS 的工作原理

MPLS 的工作原理是：为每个 IP 数据包提供一个标签，并由此决定数据包的路径以及优先级。MPLS 是一种可以在多种第二层媒体上进行标签交换的网络技术，这一技术结合了第二层的高速交换(硬件交换)和第三层的灵活路由处理的特点。

2) MPLS 的网络构成

MPLS 网络由边缘标签路由器(LER)和标签交换路由器(LSR)组成，LER 构成 MPLS 网的接入部分，LSR 构成 MPLS 网的核心部分。LER 发起或终止标签交换路径(LSP)连接并完成传统 IP 数据包转发和标签转发功能。

入口 LER 完成三项工作：将数据分组映射到 LSP 上；将数据分组封装成标签分组；将标记分组从相应端口转发出去。出口 LER 终止 LSP，并根据弹出的标签转发剩余的包。LSR 只是根据交换表完成转发功能。这样所有复杂功能都在 LER 内完成，LSR 只完成高速转发功能，如图 6-7 所示。

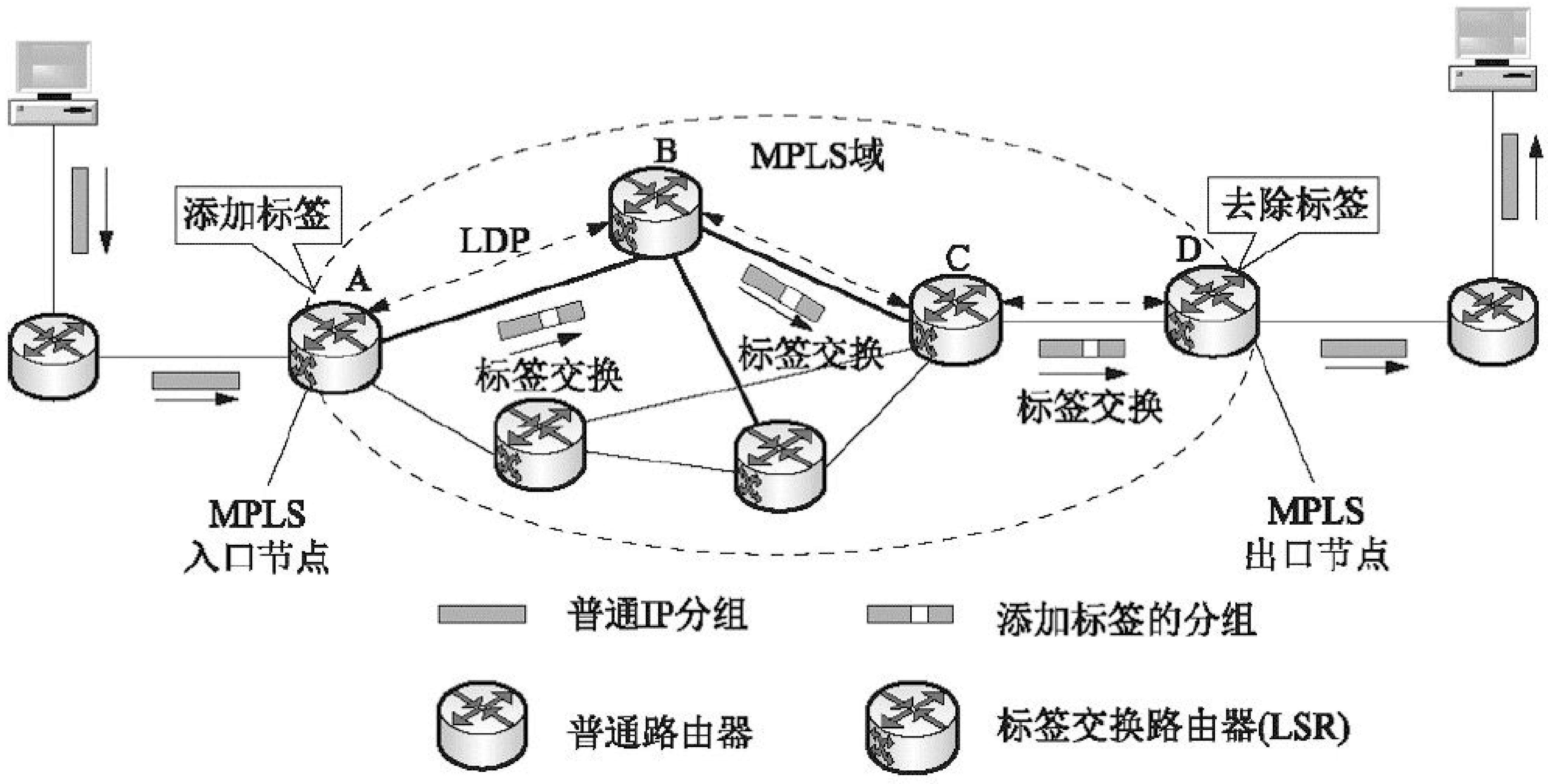


图 6-7 MPLS 的基本原理

MPLS 网络中各 LSR 通过专门标签分发协议(Label Distribution Protocol，LDP)交换报文，并找出相应的 LSP。

3) MPLS 的工作过程

MPLS 的工作过程如下。

(1) 当 IP 数据包到达 LER(标签边缘路由器)时，LER 首先分析 IP 包头的信息。对于每一个 FEC，LER 根据标签信息库(LIB)为该 IP 数据包分配一个标签，并将使用该标签封装的数据包从 LIB 所规定的下一个接口发送出去。

(2) 当带有标签的数据包到达 MPLS 网络内部 LSR 时，LSR 提取局部标签，同时使用该标签到 LIB 查找输出标签和下一个接口，并使用输出标签代替数据包的输入标签后将新数据包从下一个接口发送出去。

(3) 数据包到达 MPLS 域的另外一端，这时 LER 去掉封装的标签，仍然按照 IP 包的路由方式将数据包继续传送到目的地。

6.8.2 典型例题分析

例 6-53 使用 CIDR 技术把 4 个 C 类网络 202.15.145.0/24、202.15.147.0/24、202.15.149.0/24 和 202.15.150.0/24 汇聚成一个超网，得到的地址是 __(53)__ 。(2017 年下半年真题 53)

A. 202.15.128.0/20　　B. 202.15.144.0/21

C. 202.15.145.0/23　　D. 202.15.152.0/22

解析：将 4 条地址的第三个字节写成二进制位:

1001 0001

1001 0011

1001 0101

1001 0110

经过汇聚后前 21 位相同，故得到的地址为 202.15.144.0/21。

答案：B

例 6-54 下面是路由表的 4 个表项，与地址 220.112.179.92 匹配的表项是__(52)__。(2016 年下半年真题 52)

A. 220.112.145.32/22　　B. 220.112.145.64/22

C. 220.112.147.64/22　　D. 220.112.177.64/22

解析：地址 220.112.145.32/22 的二进制形式是 1101 1100.0111 0000.1001 0001.0010 0000

地址 220.112.145.64/22 的二进制形式是 1101 1100.0111 0000.1001 0001.0100 0000

地址 220.112.147.64/22 的二进制形式是 1101 1100.0111 0000.1001 0011.0100 0000

地址 220.112.177.64/22 的二进制形式是 1101 1100.0111 0000.1011 0001.0100 0000

而地址 220.112.179.92 的二进制形式是 1101 1100.0111 0000.1011 0011.0101 1100

所以与地址 220.112.179.92 匹配的是 220.112.177.64/22。

答案：D

例 6-55 某用户得到的网络地址范围为 110.15.0.0～110.15.7.0，这个地址块可以用__(54)__，其中可以分配__(55)__个可用主机地址。(2016 年下半年真题 54、55)

(54) A. 110.15.0.0/20　　B. 110.15.0.0/21

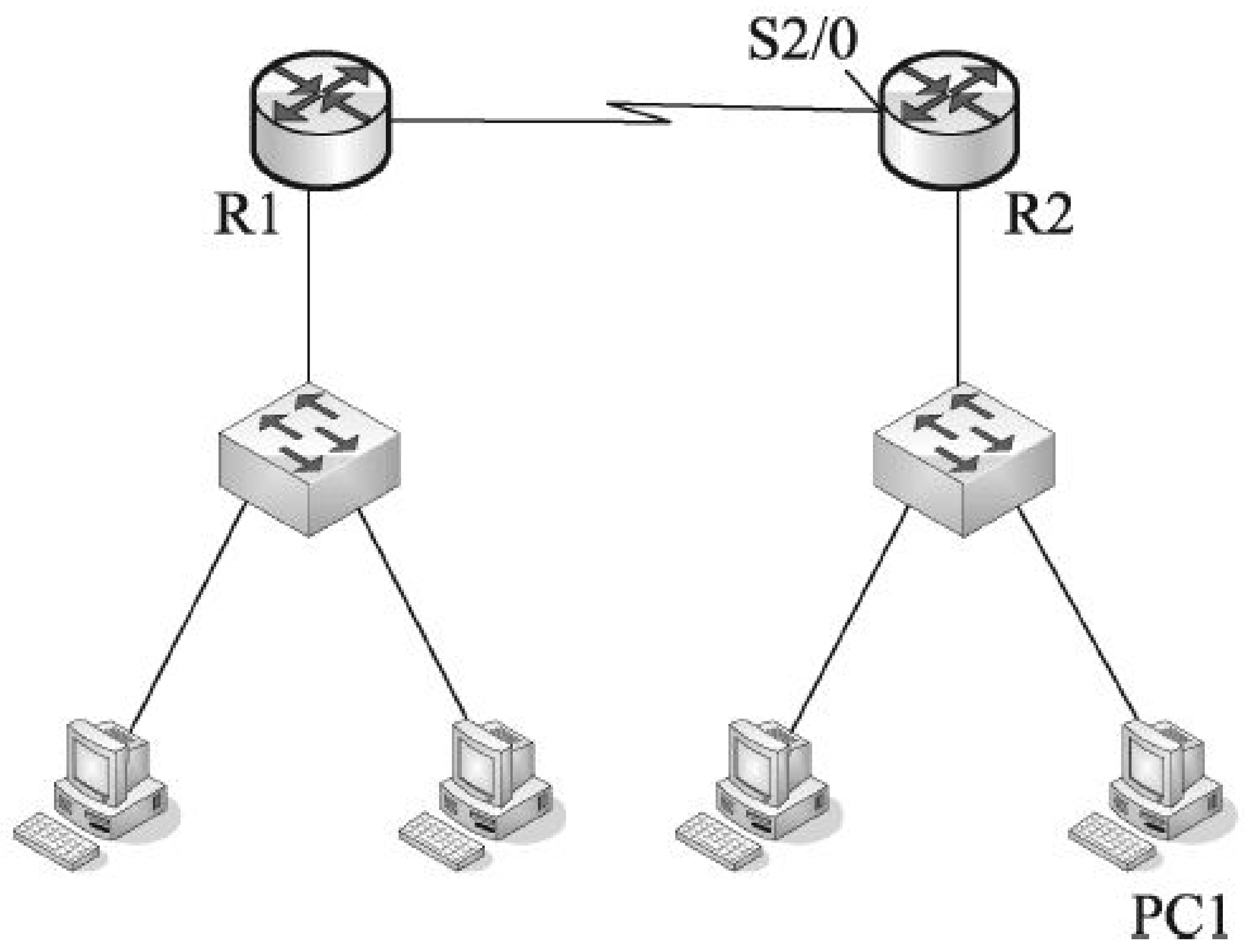
C. 110.15.0.0/16　　D. 110.15.0.0/24

(55) A. 2048　　B. 2046　　C. 2000　　D. 2056

解析：对 110.15.0.0～110.10.0000 0111.0 8 个子网进行汇聚，汇聚后掩码长度为 21 位，则主机号有 11 位，可用主机地址 $2^{11}-2=2046$ 个。

答案：(54)B　(55)B

例 6-56 某网络拓扑结构如下图所示。



在路由器 R2 上采用命令__(28)__得到如下图所示结果。PC1 可能的 IP 地址为__(29)__，路由器 R2 的 S2/0 口的 IP 地址为__(30)__。若在 PC1 上查看主机的路由表，采用的命令为__(31)__。(2016 年上半年真题 28～31)

```
R2>
    …
    R       192.168.0.0/24 [120/1] via 202.117.112.1, 00:00:11, Serial2/0
    C       192.168.1.0/24 is directly connected, FastEthernet0/0
                 202.117.112.0/30 is subnetted, 1 subnets
    C       202.117.112.0 is directly connected, Serial2/0
R2>
```

(28) A. nslookup　B. route print　C. ip routing　D. show ip route
(29) A. 192.168.0.1　B. 192.168.1.1　C. 202.117.112.1　D. 202.117.112.2
(30) A. 192.168.0.1　B. 192.168.1.1　C. 202.117.112.1　D. 202.117.112.2
(31) A. nslookup　B. route print　C. ip routing　D. show ip route

解析：在路由器上显示路由表的命令是：show ip route。

在路由器表中，C 表示直连的路由，R 表示路由器学习到的路由；路由器 R2 直连的局域网段为 192.168.1.0/24，那么 PC1 的地址就属于这一网段，路由器 R2 直连的广域网段是 202.117.112.0/30，那么 S2/0 口就属于这个网段，又因为学习到的 192.168.0.0/24 是通过下一跳也就是 R1 和 R2 相连的接口地址 202.117.112.1，则 S2/0 口的地址可以根据 202.117.112.0/30 和 202.117.112.1 算出为 202.117.112.2。

在主机上查看路由表的命令为 route print 或 netstat –r。

答案：(28) D　(29) B　(30) D　(31) B

例 6-57　假设路由表有 4 个表项如下所示，那么与地址 115.120.145. 67 匹配的表项是 __(52)__，与地址 115. 120. 179. 92 匹配的表项是 __(53)__。(2016 年上半年真题 52、53)

(52)、(53) A. 115. 120. 145. 32　B. 115. 120. 145. 64
C. 115. 120. 147. 64　D. 115. 120. 177. 64

解析：115.120.145.67 的第三和第四字节展开成二进制形式：115.120.1001 0001.0100 0011。再将 4 个选项 IP 地址的第三、四字节也展开成二进制形式，寻找最大的相同位数。

A. 115.120.1001 0001.0010 0000　B. 115.120.1001 0001.0100 0000
C. 115.120.1001 0011.0100 0000　D. 115.120.1011 0001.0100 0000

显然，匹配度最高的为选项 B。(53)同理。

答案：(52) B　(53) D

例 6-58　假设分配给用户 U1 的网络号为 192.25.16.0～192.25.31.0，则 U1 的地址掩码应该为 __(54)__；假设分配给用户 U2 的网络号为 192.25.64.0/20，如果路由器收到一个目标地址为 11000000.00011001.01000011.00100001 的数据报，则该数据报应传送给用户 __(55)__。(2016 年上半年真题 54、55)

(54) A. 255.255.255.0　B. 255.255.250.0
C. 255.255.248.0　D. 255.255.240.0

(55) A. U1　B. U2　C. U1 或 U2　D. 不可到达

解析：16 个 C 类地址进行聚合 192.25.16.0～192.25.31.0，聚合后的最大的相同位数为 20 位，那么 U1 的地址掩码应为 11111111.11111111.11110000.00000000，即 255.255.240.0，聚合后的地址为 192.25.16.0/20。分配给用户 U2 的网络号为 192.25.64.0/20，如果路由器收到一个目标地址为 11000000.00011001.01000011.00100001(192.25.67.33)的数据报，很明显该

数据包属于 U2 网络，故数据包应传送给用户 U2。

答案：(54) D　(55) B

例 6-59　通过 CIDR 技术，把 4 个主机地址 220.78.169.5、220.78.172.10、220.78.174.15 和 220.78.168.254 组织成一个地址块，则这个超级地址块的地址是__(51)__。(2015 年下半年真题 51)

A. 220.78.177.0/21　　B. 220.78.168.0/21

C. 220.78.169.0/20　　D. 220.78.175.0/20

解析：由于一个 CIDR 地址块中有很多地址，因此，路由表就利用 CIDR 地址块来查询目的网络。这种地址的聚合常称为路由聚合，它可以让路由表中一个项目可以表示原来传统分类的很多个路由。

把 4 个主机地址 220.78.169.5、220.78.172.10、220.78.174.15 和 220.78.168.254 组织成一个地址块，方法是首先转换为二进制的形式，找出最大的相同位数，作为汇聚后的网络位。

由于 220.78 一样，所以只转换第三字节。

10101001

10101100

10101110

10101000

所以最大的相同位数是 8+8+5=21，网络地址就是 202.78.168.0/21。

答案：B

例 6-60　如果在查找路由表时发现有多个选项匹配，那么应该根据__(55)__原则进行选择。假设路由表有 4 个表项如下所示，那么与地址 139.17.179.92 匹配的表项是__(56)__。(2015 年下半年真题 55、56)

(55) A. 包含匹配　B. 恰当匹配　C. 最长匹配　D. 最短匹配

(56) A. 139.17.145.32　B. 139.17.145.64　C. 139.17.147.64　D. 139.17.177.64

解析：最长匹配原则：在使用 CIDR 时，由于采用了网络前缀这种记法，IP 地址由网络前缀和主机号两部分组成，因此在路由表中的项目也要有相应的改变。这时，每个项目由“网络前缀”和“下一跳地址”组成。但是在查找路由表时可能会得到不止一个匹配结果，这样就带来一个问题：我们应当从这些结果中选择哪一条路由呢？

正确的答案是：应当从匹配结果中选择具有最长网络前缀的路由。这叫作最长前缀匹配，这是因为网络前缀越长，其地址块就越小，路由就越具体。

假设路由表有 4 个表项，如 56 题 4 个选项所示，那么与地址 139.17.179.92 匹配的表项是 139.17.177.64，因为它和 139.17.179.92 具有最多的相同位数。

答案：(55) C　(56) D

6.8.3　同步练习

1.　把下列 8 个地址块 20.15.0.0～20.15.7.0 聚合成一个超级地址块，则得到的网络地址是________。

A. 20.15.0.0/20　B. 20.15.0.0/21　C. 20.15.0.0/16　D. 20.15.0.0/24

2. NAT 技术解决了 IPv4 地址短缺的问题。假设内网的地址数是 m，外网的地址数是 n，若 $m>n$，则这种技术叫作__(1)__；若 $m>n$，且 $n=1$，则这种技术叫作__(2)__。

(1)、(2) A. 动态地址翻译　　B. 静态地址翻译
C. 地址伪装　　D. 地址变换

3. CIDR 技术解决了路由缩放问题。例如 2048 个 C 类网络组成一个地址块，网络号为 192.24.0.0～192.31.255.0，这样的超网号应为__(1)__，其地址掩码应为__(2)__。

(1) A. 192.24.0.0　　B. 192.31.255.0
C. 192.31.0.0　　D. 192.24.255.0

(2) A. 255.255.248.0　　B. 255.255.255.0
C. 255.255.0.0　　D. 255.248.0.0

6.8.4 同步练习参考答案

1. B　2. (1) A　(2) C　3. (1) A　(2) D

6.9 IP 组播技术

6.9.1 考点辅导

近年来，随着 Internet 的迅速普及和爆炸性发展，在 Internet 上产生了许多新的应用，其中不少是高带宽的多媒体应用，譬如网络视频会议、网络音频/视频广播、AOD/VOD、股市行情发布、多媒体远程教育、CSCW 协同计算、远程会诊。这就带来了带宽的急剧消耗和网络拥挤的问题。为了缓解网络瓶颈，人们提出各种方案，归纳起来，主要包括以下四种。

(1) 增加互连带宽；
(2) 服务器的分散与集群，以改变网络流量结构，减轻主干网的瓶颈；
(3) 应用 QoS 机制，把带宽分配给一部分应用；
(4) 采用 IP Multicast(译为组播、多播或多路广播，下文不加区分)技术。

比较而言，IP 组播技术有其独特的优越性——在组播网络中，即使用户数量成倍增长，主干带宽也不需要随之增加。这个优点使它成为当前网络技术中的研究热点之一。

6.9.1.1 组播网络的体系结构

组播网络的体系结构包括：组播的基本工作原理、实现组播的条件、组播的地址分配方案及与 MAC 地址映射、Internet 组管理协议。

1. 组播的工作原理

组播是一种允许一个或多个发送者(组播源)发送单一的数据包到多个接收者(一次的，同时的)的网络技术。组播源把数据包发送到特定组播组，而只有属于该组播组的地址才能

接收到数据包。组播可以大大的节省网络带宽，因为无论有多少个目标地址，在整个网络的任何一条链路上只传送单一的数据包。

(1) 单播(Unicast)传输：在发送者和每一接收者之间需要单独的数据信道。如果一台主机同时给很少量的接收者传输数据，一般没有什么问题。但如果有大量主机希望获得数据包的同一份拷贝时却很难实现。这将导致发送者负担沉重、延迟长、网络拥塞；为保证一定的服务质量需增加硬件和带宽。

(2) 组播(Multicast)传输：它提高了数据传送效率。减少了主干网出现拥塞的可能性。组播组中的主机可以是在同一个物理网络，也可以来自不同的物理网络(如果有组播路由器的支持)。

(3) 广播(Broadcast)传输：是指在 IP 子网内广播数据包，所有在子网内部的主机都将收到这些数据包。广播意味着网络向子网主机都投递一份数据包，不论这些主机是否乐于接收该数据包。然而广播的使用范围非常小，只在本地子网内有效，因为路由器会封锁广播通信。广播传输增加非接收者的开销。

2. 实现 IP 组播的前提条件

实现 IP 组播传输，则组播源和接收者以及两者之间的下层网络都必须支持组播。这包括以下几方面：

- 主机的 TCP/IP 实现支持发送和接收 IP 组播；
- 主机的网络接口支持组播；
- 有一套用于加入、离开、查询的组管理协议，即 IGMP(v1,v2)；
- 有一套 IP 地址分配策略，并能将第三层 IP 组播地址映射到第二层 MAC 地址；
- 支持 IP 组播的应用软件；
- 所有介于组播源和接收者之间的路由器、集线器、交换机及 TCP/IP 栈、防火墙均需支持组播。

目前，IP 组播技术得到硬件、软件厂商的广泛支持，比如，新生产的以太网卡几乎都支持组播；Cisco 的路由器不仅支持 DVMRP、PIM 路由协议及 IGMP 组管理协议，而且支持 Cisco 专有 Cisco 组管理协议 CGMP，再如微软的 Windows 95 支持 IP 组播和 IGMPv1，而 Windows 98 还支持 IGMPv2。对于不支持 IP 组播传输的中间路由器采用 IP 隧道(Tunneling)技术作为过渡方案。这些说明 IP 组播技术的应用环境已基本具备。

3. 组播地址分配与 MAC 地址

在组播通信中，我们需要两种地址：一个 IP 组播地址和一个 Ethernet 组播地址。其中，IP 组播地址标识一个组播组。由于所有 IP 数据包都封装在 Ethernet 帧中，所以还需要一个组播 Ethernet 地址。为使组播正常工作，主机应能同时接收单播和组播数据，这意味着主机需要多个 IP 和 Ethernet 地址。

IP 地址方案专门为组播划出一个地址范围，在 IPv4 中为 D 类地址，范围是 224.0.0.0 到 239.255.255.255，并将 D 类地址划分为局部链接组播地址、预留组播地址、管理权限组播地址；在 IPv6 中为组播地址提供了许多新的标识功能，图 6-8 所示为 IPv4 和 IPv6 的组播地址格式，其中 IPv6 中特殊域的定义如图 6-9 所示。

图 6-8　IPv4 和 IPv6 的组播地址格式

域	值	含义
flags	0000	永久组播地址
	0001	动态组播地址
scope	0001	本地节点
	0010	本地链路
	0101	本地网点
	1000	本地组织
	1110	全局组播地址
	其他	保留或未指定

图 6-9　IPv6 中特殊域的定义

局部链接地址：224.0.0.0～224.0.0.255，用于局域网，路由器不转发属于此范围的 IP 包；

预留组播地址：224.0.1.0～238.255.255.255，用于全球范围或网络协议；

管理权限地址：239.0.0.0～239.255.255.255，组织内部使用，用于限制组播范围。

1)　以太网与 FDDI 组播 MAC 地址映射

IP 组播帧都使用以 0X0100.5EXX.XXXX 的 24 位前缀开始的 MAC 层地址，但只有其中的一半 MAC 地址可以被 IP 组播使用，剩下的 MAC 地址空间的 23 位作为第三层 IP 组播地址进入第二层 MAC 地址的映射使用。由于第三层 IP 组播的 28 位地址不能映射到只有 23 位的可用 MAC 地址空间，造成有 32 个 IP 组播的地址不明确，所以主机 CPU 必须对收到的每一个组播数据包做出判断。这增加了主机 CPU 的开销。此外，还产生抑制第二层局域网交换的组播扩散问题。

2)　令牌环网组播 MAC 地址映射

令牌环网 MAC 地址格式与标准以太网 MAC 地址格式位序相反。令牌环网的缺点是其功能地址位使得它对组播地址映射的不明确性高达 228:1，这意味着令牌环网上的组播数据流将导致令牌环网点的 CPU 被环路上的每一个组播数据包中断，从这个角度来说，令牌环网不适合于组播。

4. 组播树

在单播模型中，数据包通过网络沿着单一路径从源主机向目标主机传递，但在组播模型中，组播源向某一组地址传递数据包，而这一地址却代表一个主机组。为了向所有接收者传递数据，一般采用组播分布树描述 IP 组播在网络里经过的路径。

组播分布树有四种基本类型：泛洪法、有源树、有核树和 Steiner 树。

1)　泛洪法(Flooding)

这是最简单的向前传送组播路由算法，并不构造所谓的分布树。其基本原理如下：当组播路由器收到发往某个组播地址的数据包后，首先判断是否是首次收到该数据包，如果是首次收到，那么将其转发到所有接口上，以确保其最终能到达所有接收者；如果不是首次收到，则抛弃该数据包。

泛洪法的实现关键是“首次收到”的检测。这需要维护一个最近通过的数据包列表，但无须维护路由表。它适合于对组播需求比较高的场合，并且能做到即使传输出现错误，

只要还存在一条到接收者的链路，则所有接收者都能接收到组播数据包。然而，泛洪法不适合用于 Internet，因为它不考虑链路状态，并产生大量的拷贝数据包。此外，对于高速网络而言，“首次收到”列表将会很长，占用相当大的内存；尽管它能保证不对相同的数据包进行二次转发，但不能保证对相同数据包只接收一次。

2) 有源树

有源树也称为基于信源的树或最短路径树(Shortest Path Tree，SPT)。它是以组播源为根构造的从根到所有接收者路径都最短的分布树。如果组中有多个组播源，则必须为每个组播源构造一棵组播树。由于不同组播源发出的数据包被分散到各自分离的组播树上，因此采用 SPT 有利于网络中数据流量的均衡。同时，因为从组播源到每个接收者的路径最短，所以端到端(end-to-end)的时延性能较好，有利于流量大、时延性能要求较高的实时媒体应用。SPT 的缺点是：要为每个组播源构造各自的分布树，当数据流量不大时，构造 SPT 的开销相对较大。

3) 共享树

共享树也称 RP 树(RPT)，是指为每个组播组选定一个共用根(汇合点 RP 或 核心)，以 RP 为根建立的组播树。同一组播组的组播源将所要组播的数据单播到 RP，再由 RP 向其他成员转发。目前，讨论最多同时也是最具代表性的两种共享树是 Steiner 树和有核树(CBT)。

(1) Steiner 树是总代价最小的分布树，它使连接特定图(graph)中的特定组成员所需的链路数最少。若考虑资源总量被大量的组使用的情况，那么使用资源较少最终就会减少产生拥塞的风险。Steiner 树相当不稳定，树的形状随组中成员关系的改变而改变，且对大型网络缺少通用的解决方案。所以 Steiner 树只是一种理论模型，而非实用工具。目前，出现了许多 Steiner 树的次优启发式生成算法。

(2) 有核树是由根到所有组成员的最短路径合并而成的树。

共享树在路由器所需存储的状态信息的数量和路由树的总代价两个方面具有较好的性能。当组的规模较大，而每个成员的数据发送率较低时，使用共享树比较适合。但当通信量大时，使用共享树将导致流量集中及根(RP)附近的瓶颈。

5. 组管理协议 IGMP

主机使用 IGMP 通知子网组播路由器，希望加入多播组；路由器使用 IGMP 查询本地子网中是否有属于某个组播组的主机。

1) 加入多播组

当某个主机加入某一个多播组时，它通过“成员资格报告”消息通知它所在的 IP 子网的组播路由器，同时将自己的 IP 模块做相应的准备，以便开始接收来自多组播组传来的数据。如果这台主机是它所在的 IP 子网中第一台加入该多播组的主机，通过路由信息的交换，组播路由器加入组播分布树。

2) 退出多播组

在 IGMP v1 协议中，当主机离开某一个多播组时，它将自行退出。组播路由器定时(如 120 秒) 使用“成员资格查询” 消息向 IP 子网中的所有主机的组地址(224.0.0.1)查询，如果某一组播组在 IP 子网中已经没有任何成员，那么组播路由器在确认这一事件后，将不再在子网中转发该多播组的数据。与此同时，通过路由信息交换，从特定的多播组分布树中删除相应的组播路由器。这种不通知任何人而悄悄离开的方法，使得组播路由器知道 IP 子网

中已经没有任何成员的事件延时了一段时间，所以在 IGMP v2.0 中，当每一个主机离开某一个多播组时，需要通知子网组播路由器，组播路由器立即向 IP 子网中的所有多播组询问，从而减少了系统处理停止组播的延时。

6.9.1.2　组播转发

由于组播源是向多播组发送数据包而非单播模型中的具体目标主机，所以组播路由器不能依靠 IP 包中的目标地址来决定如何转发数据包，而必须将组播数据包转发到多个外部接口上，以便同一多播组的成员都能接收到数据包。这使组播转发比单播转发更加复杂。大多数现有组播路由协议使用逆向路径转发(RPF)机制作为组播转发的基础。

1. 逆向路径转发(Reverse Path Forward，RPF)

当组播数据包到达路由器时，路由器作 RPF 检查，以决定是否转发或抛弃该数据包，若成功则转发，否则抛弃。

RPF 检查过程如下。

检查数据包的源地址，以确定该数据包经过的接口，是否在从源到此的路径上；

若数据包是从可返回源主机的接口上到达，则 RPF 检查成功，转发该数据包到输出接口表上的所有接口；否则 RPF 检查失败，抛弃该数据包。

2. 组播转发缓存

对于每一个输入组播数据包进行 RPF 检查会导致较大的路由器性能损失。因此，建立组播转发缓存时，通常由组播路由确定 RPF 接口。然后将 RPF 接口变成组播转发缓存项的输入接口。一旦 RPF 检查程序使用的路由表发生变化，必须重新计算 RPF 接口；并更新组播转发缓存项。

3. TTL 阈值

每当路由器转发组播数据包，IP 包中的 TTL(Time To Live)值都减 1。若数据包的 TTL 减少到 0，则路由器将抛弃该数据包。TTL 阈值可用于组播路由器的各个接口，以防止在该接口上转发低于 TTL 阈值的组播数据包。这样可对组播的范围加以控制。表 6-4 给出典型的初始 TTL 值和作为不同 TTL 边界的路由器接口 TTL 阈值。

表 6-4　典型的 TTL 边界值

范　围	初始 TTL 值	TTL 阈值
本地网	1	N/A
区域	15	16
地区	63	64
全球	127	128

4. 管理权限边界

除 TTL 阈值外，组播提供另一种称为管理权限的地址机制作为边界，以限制组播信息转发到域外。管理权限的组播地址是从 239.0.0.0 到 239.255.255.255，这段地址被认为是本地分配(类似于单播中的 192.168.xx.xx)，不能用于 Internet。这种机制使得在 Intranet 内部可

重复使用组播地址，提高组播地址空间的利用率。

6.9.1.3 组播路由协议

要想在一个实际网络中实现组播数据包的转发，必须在各个互连设备上运行可互操作的组播路由协议。组播路由协议可分为三类：密集模式协议(如 DVMRP，PIM-DM)、稀疏模式协议(如 PIM-SM，CBT)和链路状态协议 (MOSPF)，下面分别介绍各个协议的工作原理。

1. 距离向量组播路由协议(Distance Vector Multicast Routing Protocol，DVMRP)

DVMRP 由单播路由协议 RIP 扩展而来，两者都使用距离向量算法得到网络的拓扑信息，不同之处在于 RIP 根据路由表前向转发数据，而 DVMRP 则是基于 RPF。为了使新加入的组播成员能及时收到组播数据，DVMPR 采用定时发送数据包给所有的 LAN 的方法，然而这种方法导致大量路由控制数据包的扩散，这部分开销限制了网络规模的扩大。另一方面，DVMRP 使用跳数作为计量尺度，其上限为 32 跳，这对网络规模也是一个限制。目前提出了分层 DVMRP，即对组播网络划分区域，在区域内的组播可以按照任何协议进行，而对于跨区域的组播则由边界路由器在 DVMRP 协议下进行，这样可大大减少路由开销。

2. 开放式组播最短路径优先协议(Multicast Open Shortest Path First，MOSPF)

MOSPF 是一种基于链路状态的路由协议，是对单播 OSPF 协议的扩展。

同 OSPF 类似，MOSPF 定义了三种级别的路由。

① MOSPF 区域内组播路由：用于了解各网段中的组播成员，构造(源网络 S，组 G)对的 SPT；

② MOSPF 区域间组播路由：用于汇总区域内成员关系，并在自治系统(AS)主干网(区域 0)上发布组成员关系记录通告，实现区域间组播包的转发。

③ MOSPF AS 间组播路由：用于跨 AS 的组播包转发。

区域内 MOFPF 利用了链路状态数据库，对单播 OSPF 数据格式进行扩充，定义了新的链路状态通告(Link State Advertisement，LSA)，使得 MOSPF 路由器了解哪些多播组在哪些网络上。路由器使用 Dijkstra 算法构造(源网络 S，组 G)对的 SPT。MOSPF 与 DVMRP 相比，路由开销较小，链路利用率高，然而 Dijkstra 算法计算量很大，为了减少路由器的计算量，MOSPF 执行一种按需计算方案，即只有当路由器收到组播源的第一个组播数据包后，才对(S，G)SPT 计算，否则利用转发缓存(cache)中的(S，G)SPT。

MOSPF 继承了 OSPF 对网络拓扑的变化响应速度快的优点，但拓扑变动使所有路由器的缓存失效重新计算 SPT，因而消耗大量路由器 CPU 资源。这就决定了 MOSPF 不适合高动态性网络(组成员关系变化大、链路不稳定)，而适用于网络连接状态比较稳定的环境。另外，对于有大量组播源子网络的网络而言，MOSPF 的扩展性问题引起了人们的关注，有待于进一步研究。

3. 协议无关组播(Protocol Independent Multicast，PIM)

PIM 由 IDMR(域间组播路由)工作组设计，顾名思义，PIM 不依赖于某一特定单播路由协议，它可利用各种单播路由协议建立的单播路由表完成 RPF 检查功能，而不是维护一个分离的组播路由表实现组播转发。由于 PIM 无须收发组播路由更新，所以与其他组播协议相比，PIM 开销降低了许多。PIM 的设计出发点是在 Internet 范围内同时支持 SPT 和共享树，

并使两者之间灵活转换，因而集中了它们的优点提高了组播效率。PIM 定义了两种模式：密集模式(Dense-Mode，DM)和稀疏模式(Sparse-Mode，SM)。

1)　PIM-DM

PIM-DM 与 DVMRP 很相似，都属于密集模式协议，都采用了“扩散/剪枝”机制，如图 6-10 所示。同时，假定带宽不受限制，每个路由器都想接收组播数据包。主要不同之处在于 DVMRP 使用内建的组播路由协议，而 PIM-DM 采用 RPF 动态建立 SPT。

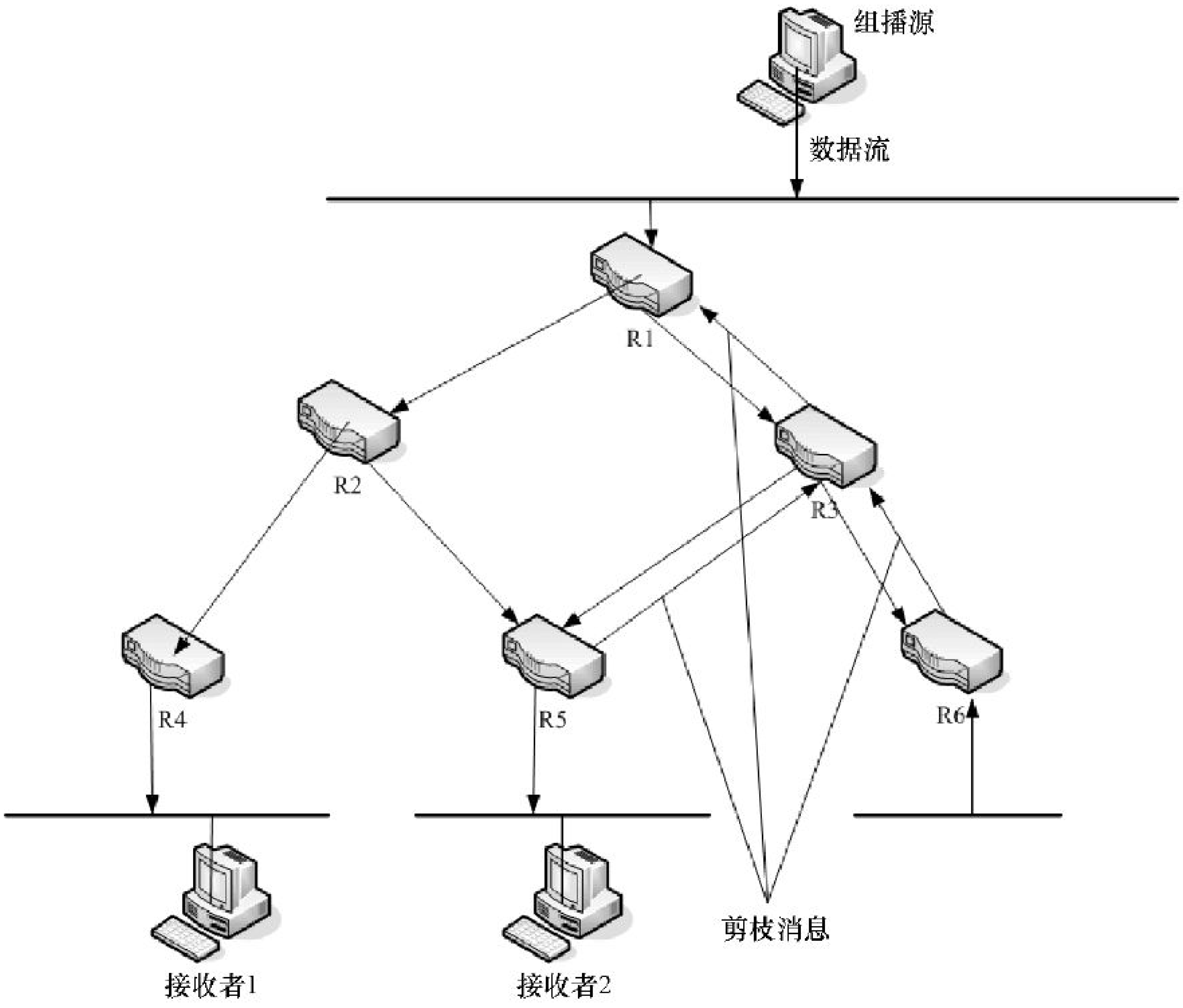


图 6-10　PIM-DM 模式示意

该模式适合于下述几种情况：高速网络；组播源和接收者比较靠近，发送者少，接收者多；组播数据流比较大且比较稳定。

2)　PIM-SM

PIM-SM 与基于“扩散/剪枝”模型的根本差别在于 PIM-SM 是基于显式加入模型，即接收者向 RP 发送加入消息，而路由器只在已加入某个多播组输出接口上转发那个多播组的数据包。

PIM-SM 采用共享树进行组播数据包转发。每一个组有一个汇合点(Rendezvous Point，RP)，组播源沿最短路径向 RP 发送数据，再由 RP 沿最短路径将数据发送到各个接收端，如图 6-11 所示。这一点类似于 CBT，但 PIM-SM 不使用核的概念。PIM-SM 主要优势之一是它不局限于通过共享树接收组播信息， 还提供从共享树向 SPT 转换的机制。

尽管从共享树向 SPT 转换减少了网络延迟以及在 RP 上可能出现的阻塞，但这种转换耗费了相当的路由器资源，所以它适用于有多对组播数据源和网络组数目较少的环境。

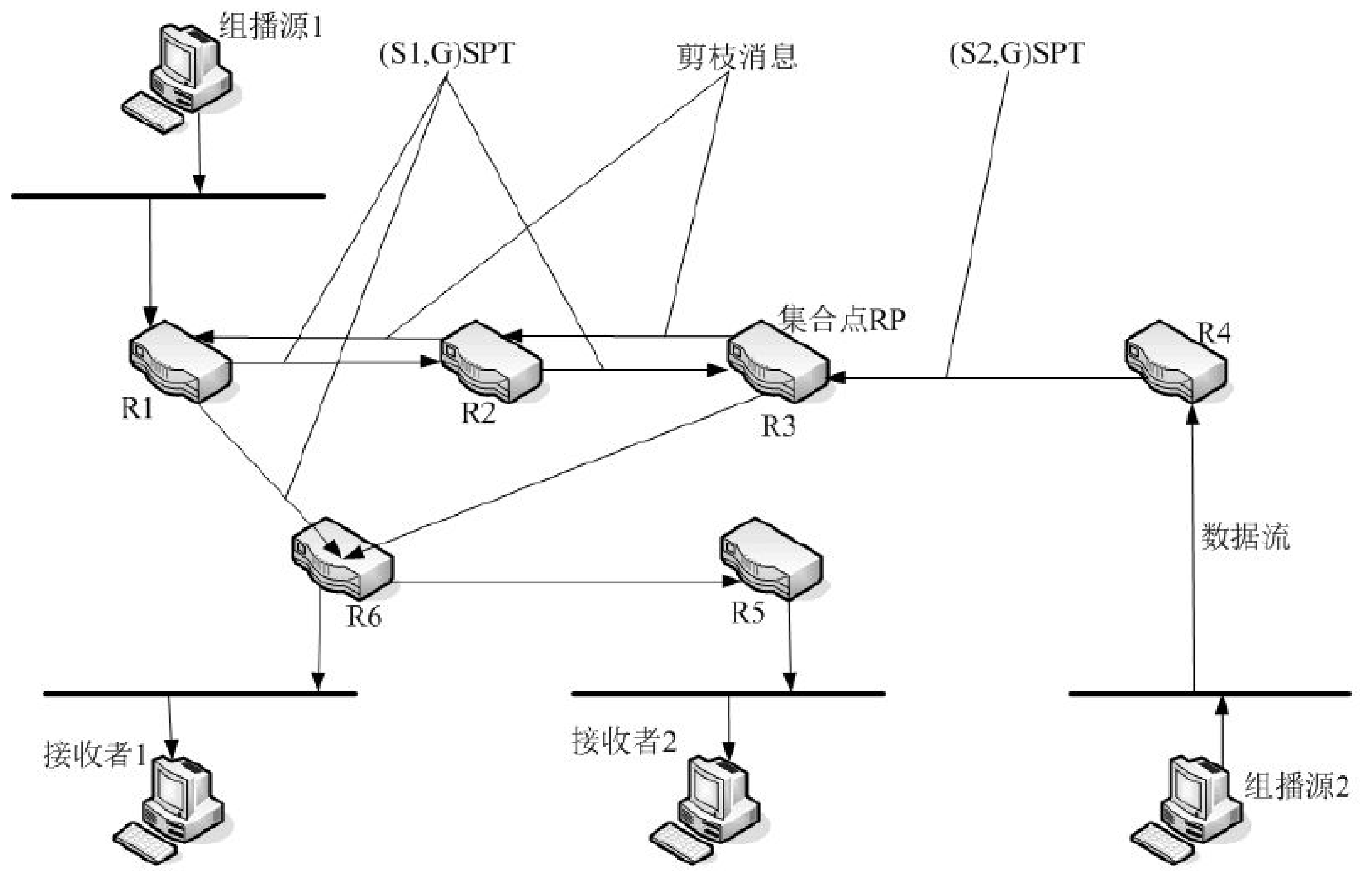


图 6-11　PIM-SM 模式示意

4. 有核树组播路由协议(Core-Based Trees，CBT)

CBT 的基本目标是减少网络中路由器组播状态，以提供组播的可扩展性。为此，CBT 被设计成稀疏模式(与 PIM-SM 相似)。CBT 使用双向共享树，双向共享树以某个核心路由器为根，允许组播信息在两个方向流动。这一点与 PIM-SM 不同(PIM-SM 中共享树是单向的，在 RP 与组播源之间使用 SPT 将组播数据转发到 RP)，所以 CBT 不能使用 RPF 检查，而使用 IP 包头的目标组地址作检查转发缓存。这就要求对 CBT 共享树的维护非常小心，以确保不会产生组播路由循环。

从路由器创建的组播状态的数量来看， CBT 比支持 SPT 的协议效率高，在具有大量组播源和组的网络中，CBT 能把组播状态优化到组的数量级。

CBT 为每个组播组建立一个生成树，所有组播源使用同一棵组播树。CBT 工作过程大体如下。

(1) 首先选择一个核，即网络中多播组的固定中心，来构造一棵 CBT。

(2) 主机向这个核发送 join 命令。

(3) 所有中间路由器都接收到该命令，并把接收该命令的接口标记为属于这个组的树。

(4) 如果接收到命令的路由器已是树中一个成员，那么只要再标记一次该接口属于该组；如果路由器第一次收到 join 命令，那么它就向核的方向进一步转发该命令，路由器就需要为每个组保留一份状态信息。

(5) 当组播数据到达一个在 CBT 树上的组播路由器时，路由器组播数据到树的核。以保证数据能够发送到组的所有成员。

CBT 将组播扩张限制在接收者范围内，即使第一个数据包也无须在全网扩散，但 CBT 导致核周围的流量集中，网络性能下降。所以某些版本的 CBT 支持多个核心以平衡负载。

目前 CBTv3 草案已公布。该方案通过使用 CBT 边界路由器(BR)更好地处理域间组播的转发。CBTv3 还引入新的状态及单向分支 CBT 概念。尽管 CBT 很有代表性，但至今却几乎没有已实现的 CBT 网络。

6.9.2　典型例题分析

例 6-61　关于 IP 组播技术的描述中，错误的是________。

A. 采用组播地址寻址

B. 可使用 CGMP 协议

C. 多播组中的成员是动态的

D. 必须底层硬件支持

解析：IP 组播的特点是：组播使用组地址、动态的组成员、底层硬件支持的组播。其中底层硬件支持的组播是指当底层是支持硬件组播的网络如以太网，就利用硬件进行组播，并不是必须底层硬件支持才能使用组播方式。

CGMP 是组播协议。所以本题选 D。

答案：D

6.9.3　同步练习

下面____不是组播地址。

A. 224.0.1.1　　B. 232.0.0.1　　C. 233.255.255.1　　D. 240.255.255.1

6.9.4　同步练习参考答案

D

6.10　IP QoS 技术

6.10.1　考点辅导

1. 集成服务

集成服务模型的基本思想是将 RSVP (Resource reSerVation Protocol，资源预留协议)作为 Int-Serv 结构中的主要信令协议，它基于每个流提供端到端的保证或是受控负载的服务。Int-Serv 使用一种类似 ATM 的 SVC(Switched Virtual Circuit，交换虚电路)的方法，它在发送方和接收方之间用 RSVP 作为每个流的信令。RSVP 信息跨越整个网络。

这种服务模型在发送报文前，需要向网络申请特定的服务。应用程序先通知网络发送报文的流量参数和所需的服务质量请求(如带宽、时延等)，应用程序在收到网络预留资源的确认信息后，才开始发送报文，发送报文被控制在流量参数规定的范围内。

集成服务模型的优点如下：它具有很好的 QoS 保证，由于引入了 RSVP 协议，因此可以知道网络状态的动态改变，如设备相邻节点的退出和加入，从而可实现网络资源更加有

效地分配。

集成服务模型的缺点如下：网络的扩展性不好，随着网络的扩大，业务流的增加，每一个使用这种 QoS 技术的节点的负担会越来越大。

2. 区分服务

区分服务模型的基本思想是可以根据预先确定的规则对数据流进行分类，以便将多种应用数据流综合为有限的几种数据流等级。

区分服务是由综合服务发展而来的，它采用了 IETF 的基于 RSVP 的服务分类标准，抛弃了分组流沿路节点上的资源预留。

IP QoS 的业务区分结构使用 IPv4 报头中的业务类型(ToS)字段，并将 8 位 ToS 字段重新命名，作为 DS 字段，其中 6 位可供目前使用，其余 2 位以备将来使用。

Diff-Serv 将整个网络分成若干个域。在 Diff-Serv 域中，节点大致分为以下两类，即边缘节点和内部节点。其中边缘节点根据数据流的方向分为入口边缘节点和出口边缘节点，如图 6-12 所示。在入口处根据用户业务等级协定(SLA)，分类并标志输入的每个业务包，对每个 IP 包指定一个类型以标志 DSCP(Diff-Serv 代码点)，并分别将其排入相应的队列。内部节点负责查看 DSCP 值，将进入的数据包按级别排队，并按事先设定的带宽缓冲处理，进行下一跳转发(PHB)。

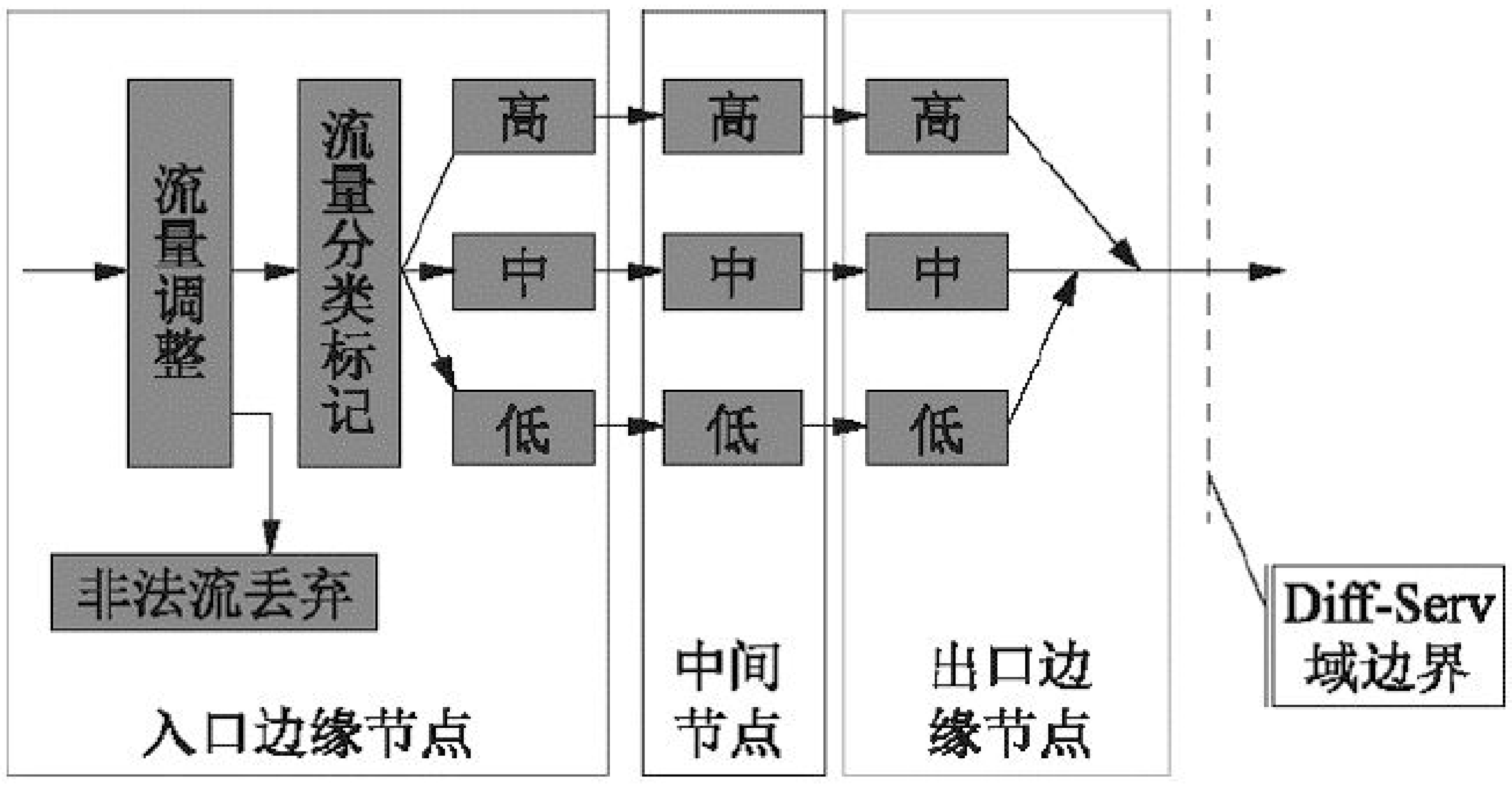


图 6-12　Diff-Serv 域中节点分类

IPv4 包的 ToS 字段定义如图 6-13 所示。

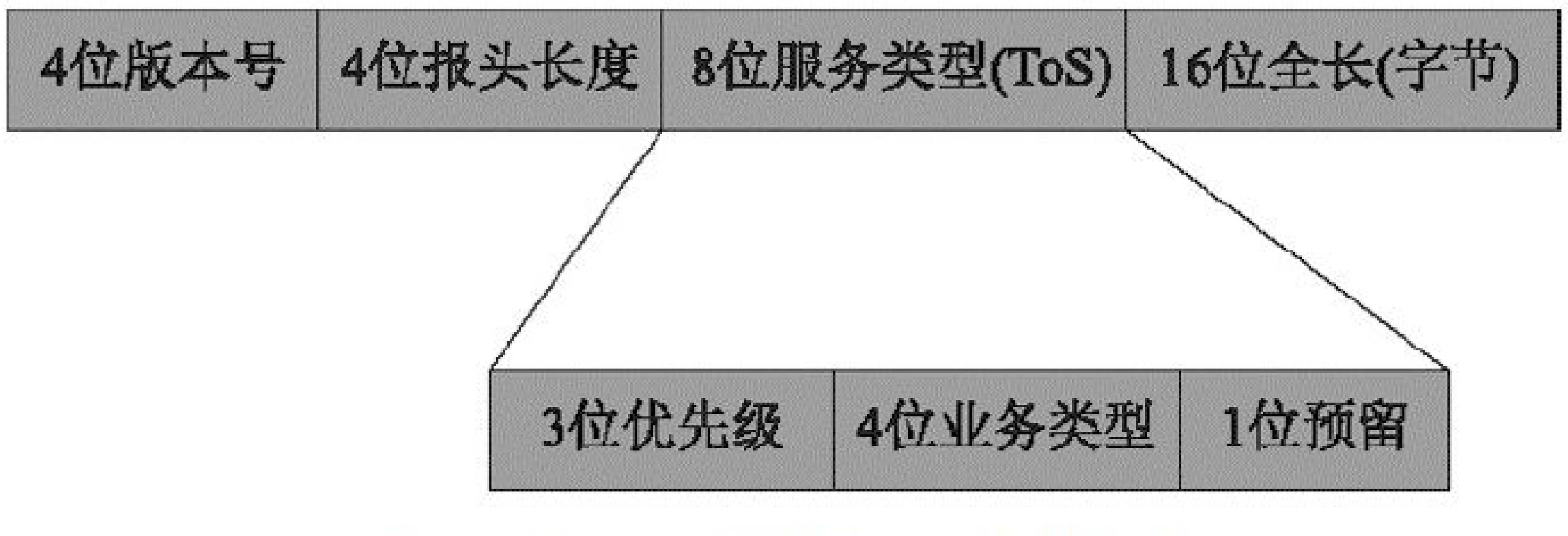


图 6-13　IPv4 包的 ToS 字段定义

Diff-Serv 也定义了 3 种业务类型。

- 尽力而为的业务(Best Effort)：类似于目前 Internet 中尽力而为的业务。
- 最优的业务(Premium)：类似于传统运营商网络的专线业务。
- 分等级的业务(Tiered)：这一类别的业务严格讲不仅仅是一种业务，而是一个大的

类别，可以根据发展的需要制定不同的业务等级。

区分服务模型的优点如下。

- 可扩展性好：DS 字段只是规定了有限数量的业务级别，状态信息的数量正比于业务级别，而不是流的数量。
- 便于实现：在网络的边界上才需要复杂的分类、标记、管制和整形操作，因此实现和部署区别型业务都比较容易。

3. 流量工程

流量工程为业务流选择路径的处理过程，以在网络中不同的链路、路由器和交换机之间平衡业务流负载。

利用多协议标签交换(Multi-Protocol Label Switching，MPLS)技术，可以协助解决 QoS 问题。MPLS 是一种结合第二层和第三层的交换技术，引入了基于标签的机制，把路由选择和数据转发分开，由标签来规定一个分组通过网络的路径。MPLS 网络由核心部分的标签交换路由器(LSR)、边缘部分的标签边缘路由器(LER)组成。

由于 MPLS 采用标签交换来进行 MPLS 转发，因此其转发效率高于传统 IP 通过路由器的转发，从而通过减少转发时间来提高 QoS。此外，MPLS 的报文头中包含一个 3bit 的 EXP 字段，通过该字段可以标记该 MPLS 报文的优先级，从而使设备在转发该 MPLS 报文时能根据优先级标志进行区别对待。

6.10.2　典型例题分析

例 6-62　多协议标记交换(MPLS)是 IETF 提出的第三层交换标准，以下关于 MPLS 的叙述中，正确的是__(67)__。(2015 年下半年真题 67)

A. 带有 MPLS 标记的分组封装在 PPP 帧中传输

B. 传送带有 MPLS 标记的分组之前先要建立对应的网络连接

C. 路由器根据转发目标把多个 IP 流聚合在一起组成转发等价类

D. MPLS 标记在各个子网中是特定分组的唯一标识

解析：MPLS 是利用标记(label，也称标签)，进行数据转发的。当分组进入网络时，要为其分配固定长度的短的标记，并将标记与分组封装在一起，在整个转发过程中，交换节点仅根据标记进行转发。

有 MPLS 标记的分组不但可以封装在 PPP 帧中传送，还可以封装在以太网、ATM 和帧中继。

MPLS 标记具有局部性，一个标记只是在一定的传输域中有效。

以太网传输数据帧，没有建立连接的概念。

答案：C

例 6-63　下列不是集成服务模型的优点的是________。

A. 它具有很好的 QoS 保证　　B. 可以知道网络状态的动态改变

C. 实现网络资源更加有效的分配　　D. 网络的扩展性好

解析：集成服务模型的缺点是网络的扩展性不好。

答案：D

6.10.3 同步练习

1. 按照 IETF 定义的区分服务(Diff-Serv)技术规范，边界路由器要根据 IP 协议头中的________字段为每个 IP 分组打上一个称为 DS 码点的标记，这个标记代表了该分组的 QoS 需求。

A. 目标地址　　B. 源地址　　C. 服务类型　　D. 段偏置值

2. 下列不属于 Diff-Serv 定义的 3 种业务类型的是________。

A. 尽力而为的业务　　B. 最优的业务

C. 分等级的业务　　D. 分层次的业务

6.10.4 同步练习参考答案

1. C　2. D

6.11 Internet 的应用

6.11.1 考点辅导

6.11.1.1 远程登录

远程登录(Telnet)是 ARPAnet 最早的网络协议之一，今天仍然有广泛的应用。该协议提供了访问远程主机的功能，使本地用户可以通过 TCP 连接登录到远程主机，像使用本地主机一样使用远程主机的资源。在本地终端与远程主机具有异构性时，也不影响它们之间的相互操作。

终端与主机之间的异构性表现在对键盘字符的解释不同。例如，PC 键盘与 IBM 大型机的键盘可能相差很大，如使用不同的回车换行符、不同的中断键等。为了使异构性的机器之间能够互操作，Telnet 定义了网络虚拟终端(NVT)。NVT 代码包括标准的 7 位 ASCII 字符集和 Telnet 命令集，这些字符和命令提供了本地终端和远程主机之间的网络接口。

Telnet 采用客户机/服务器工作方式。用户终端运行 Telnet 客户机程序，远程主机运行 Telnet 服务器程序。客户机程序与服务器程序之间执行 Telnet NVT 协议，而在两端则分别执行各自的操作系统功能。

Telnet 提供一种机制，即允许客户机程序和服务器程序协商双方都能接受的操作选项，并提供一组标准选项用于迅速建立需要的 TCP 连接。另外，Telnet 对称地对待连接的两端，并不是专门固定一端为客户机端，另一端为服务器端，而是允许连接的任一端与客户机程序相连，另一端与服务器程序相连。

Telnet 服务器可以应付多个并发的连接。通常，Telnet 服务进程等待新的连接，并为每一个连接请求产生一个新的进程。当远程终端用户调用 Telnet 服务时，终端机器上就产生

一个客户机程序，客户机程序与服务器的固定端口(23)建立 TCP 连接，实现 Telnet 服务。客户机程序接收用户终端的键盘输入，并发送给服务器；同时服务器送回字符，通过客户机软件的转换显示在用户终端上。用户就是通过这样的方式来发送 Telnet 命令，进而调用服务器主机的资源完成计算任务。

6.11.1.2　文件传输协议

文件传输协议(FTP)是 Internet 最早的应用层协议。该协议用于主机间传送文件，主机类型可以相同，也可以不同，还可以传送不同类型的文件，例如，二进制文件或文本文件等。

FTP 采用客户机/服务器工作方式。客户机与服务器之间建立两条 TCP 连接：一条用于传送控制信息，一条用于传送文件内容。FTP 的控制连接使用 Telnet 协议，主要是利用 Telnet 提供的简单的身份认证系统，供远程系统鉴别 FTP 用户的合法性。

FTP 服务器软件的具体实现依赖于操作系统。一般情况是在服务器一侧运行后台进程 S，等待出现在 FTP 专用端口(21)上的连接请求。当某个客户机向这个专用端口请求建立连接时，进程 S 便激活一个新的 FTP 控制进程 N，处理进来的连接请求。然后 S 进程返回，等待其他客户机访问。进程 N 通过控制连接与客户机进行通信，要求客户机在进行文件传送之前输入登录标识符和口令字。如果登录成功，用户可以通过控制连接列出远程目录，设置传送方式，指明要传送的文件名。当用户获准按照所要求的方式传送文件之后，进程 N 激活另一个辅助进程 D 来处理数据传送。D 进程主动开通第二条数据连接(端口号为 20)，并在文件传送完成后立即关闭此连接，D 进程也自动结束。如果用户还要传送另一个文件，再通过控制连接与 N 进程会话，请求另一次传送。

FTP 是一种功能很强的协议，除了从服务器向客户机传送文件外，还可以进行第三方传送。这时客户机必须分别开通同两个主机(比如 A 和 B)之间的控制连接。如果客户机获准从 A 机传出文件和向 B 机传入文件，则 A 服务器程序就建立一条到 B 服务器程序的数据连接。客户机保持文件传送的控制权，但不参与数据传送。

FTP 提供的命令十分丰富，包括文件传送、文件管理、目录管理、连接管理等一般文件系统具有的操作功能，还可以用 help 命令查阅各种命令的使用方法。

6.11.1.3　简单邮件传输协议

在众多的网络应用中，电子邮件系统是应用最广泛、最有发展前途的网络应用之一。据统计，在 Internet 中 1/3 以上的应用是关于电子邮件系统。电子邮件系统既是一种通用的网络应用，也是一种为其他应用所使用的基础设施。

1. 电子邮件的概念

电子邮件系统是在一些特定的节点计算机上运行相应的软件，使之充当“邮局”，用户可以在这台计算机上租用一个“电子邮箱”作为收发信件使用。电子邮件是 Internet 上使用最广泛的一种服务，它与传统的邮件最大的不同点是没有纸张，不需要写信封、贴邮票，也没有邮差，只要知道接收方的电子信箱，就可以通过计算机网络进行通信。

电子邮件的内容大多为文本格式，也可以是图形或二进制文件(程序、数据库、字处理文件)。这些特殊数据在传送之前必须转化成相应的文本信息。目前，电子邮件还可以传送

照片、声音和视频动画。电子邮件采用存储与转发技术。存储是指发送方将信息存入存储系统；当接收方准备好以后，信息就可以转发过去。邮件的发送方式可以是个人到个人、PC 到 PC 以及程序到程序等各种形式。写信人一旦将信件准备好，E-mail 软件就通过 Internet 将信件送到接收者的信箱中。

使用电子邮件必须具备以下条件。

- 用户使用的计算机必须联网。向本地服务器以外发送电子邮件，本地服务器必须与 Internet 相接。
- 邮件的发送者、接收者都必须有一个电子邮件信箱地址。
- 安装有电子邮件发/收所用的程序，如常用的 Elm、Pegasus、Pine 及 Eudora 等用户代理程序。

为了实现全球范围内的通信，用户所选用的电子邮件系统应能处理不同的邮件格式、不同的邮件地址和不同的邮件功能。

2. 电子邮箱的功能

Internet 上的电子邮件为用户提供了进行复杂通信和交互的服务功能。常用的功能如下。

- 用户的邮件可以发送给一个或多个接收者。当用户发送邮件给其他人时，只需在“CC：”列表中加入一个或多个地址。
- 电子邮件系统允许用户使用邮箱存储邮件，该功能用来存储用户一时还来不及阅读的邮件，从而可以组织大型的邮件。
- 邮件转发功能可以使用户收到信件后转发给本地服务器的各用户，也可以转发给与 Internet 联网的用户。
- 通信录和别名的使用使电子邮件的应用更加简单，电子邮件系统支持从所收到的邮件中使用邮件地址别名的功能。
- 对于比较重要的邮件，电子邮件系统可提供加密服务功能。
- 邮件的内容可以是文字、声音、图像或图形信息。
- 通过电子邮件访问 Internet 上的其他服务。

3. 电子邮箱的地址

在电子邮件发送前，每个用户必须有一个电子邮箱来存放邮件。每个电子邮箱有一个唯一的邮件地址，当用户发送邮件时，应使用电子邮件地址来说明接收方。一种广泛使用的格式是 mailbox@computer，这里 mailbox 是一个指明用户邮箱的字符串，而 computer 是一个指明邮箱所在的计算机的字符串，即域名。

将电子邮件地址划分为两部分是很重要的。因为这种划分允许每个计算机系统规定邮箱的标识，不同的计算机可以使用不同的邮箱标识机制，同时这种划分允许任一计算机系统上的用户交换电子邮件信息。为此，发送方计算机上的电子邮件软件在发送信息时使用地址中的第二部分，一旦信息到达接收方的计算机，这台计算机的本地软件就使用地址中的第一部分来选择指定的邮箱将信息放进去。

总之，每个电子邮箱都有一个唯一的地址，它分为两部分：第一部分标识用户的邮箱，第二部分标识邮箱所在的计算机。发送方的电子邮件软件使用第二部分来选择目的地，接收方的电子邮件软件使用第一部分来选择指定的邮箱。

地址的邮箱部分使用怎样的格式，取决于计算机上的电子邮件软件，也取决于使用的操作系统。有些软件系统允许系统管理员选择邮箱名字，而另一些系统需要一个与用户登录标识相同的邮箱标识。

具有选择权的系统管理员经常以将用户的姓和名字缩写的方式生成邮箱标识，这种缩写方式使得电子邮件地址中的邮箱部分容易记忆和正确输入；而使用用户登录标识构成邮箱标识的系统，邮件地址不容易读懂和记住。

4. 电子邮件信息格式

电子邮件的信息格式很简单。信息包括两部分，中间用一个空行分隔。第一部分是一个报头，包括有关发送方、接收方、信息主题等方面的信息；第二部分是主体，包括信息的文本。

虽然信息的主体可以包括任意的文本，但电子邮件软件在收、发信息时仍使报头保持标准形式。每个报头首先是一个关键字、一个冒号，然后是附加的信息。关键字告诉电子邮件软件如何翻译该行中剩下的内容。

有些关键字在电子邮件报头中是必需的，另一些是可选的。例如，每个报头必须包含以 To 开头的行，说明一个接收方的列表。To 和随后的冒号之后的内容包含一个或多个电子邮件地址，每个地址对应一个接收方。电子邮件的头部放置一个以 From 开头的行，其后跟随的是发送方的电子邮件地址。此外，还可以在后面列出一些附加信息行。表 6-5 列出了电子邮件中的一些常用关键字及其含义。

表 6-5　电子邮件常用关键字及含义

关 键 字	含　义
From	发送方地址
To	接收方地址
CC	复制副本地址
Date	信息发送日期
Subject	信息主题
Reply To	回复的地址
X-Charset	使用的字符集
X-Mailer	发送信息所使用的软件
X-Sender	发送方地址的副本

5. 邮件传输的运行方式

用户写完一个电子邮件信息并指定接收方以后，电子邮件软件将该信息的副本发送给每个接收方。在大多数系统中，需要两部分独立的程序：用户在写信息或读接收到的信息时与电子邮件接口程序进行交互；邮件传输程序将一个信息副本发送给一台远程计算机。当用户写完一个发送的信息时，电子邮件接口程序将该信息置于一个队列中由邮件传输程序处理。邮件传输程序等待放入队列的信息，然后向每个接收方发送该信息的副本。向本地计算机上的接收方发送信息副本是简单的，因为传输程序只要向用户邮箱中输入该副本就可以了。向远程用户发送副本相对复杂一些，邮件传输程序作为一个客户与远程的服务

器通信，客户向服务器发送信息，服务器将信息副本放入接收方的邮箱。

Internet 的邮件传输标准为 SMTP，即简单邮件传输协议。当邮件传输程序与远程服务器通信时，它构造一个 TCP 连接，并在此上面进行通信。一旦连接建立，这两个程序就遵循 SMTP 协议，它允许发送方指定接收方以及传输电子邮件信息。

尽管邮件传输看起来很简单，但 SMTP 协议仍需处理许多细节。例如，SMTP 要求可靠的传递，发送方必须保存一个信息的副本，直至接收方接收到该邮件副本。此外，SMTP 还允许发送方询问一个给定的邮箱在服务器所在的计算机上是否存在。

电子邮件具有分发、列表和转发功能。许多电子邮件系统包含一个邮件转发器，它是一个能转发信息副本的程序。通过邮件列表可以向一组电子邮件地址发送信件。发送方不需列出所有接收方的地址，就能向一组用户发送信件。接收方要想接收到发往该组的邮件，就必须请求在列表中加上自己的电子邮件地址。

TCP/IP 协议簇包含一个提供对电子邮件邮箱进行远程存取的协议，称为邮局协议(POP)。电子邮箱放在一台运行 POP 协议的服务器上，服务器的客户可实现对邮箱的邮件存取。POP 协议对于拨号连接的用户特别适用，用户只需与邮箱所在的计算机建立一个拨号连接，就可以与服务器进行通信，收发电子邮件。

上面介绍的 SMTP 协议与相应的电子邮件服务器和 POP 协议与 POP 服务器，它们是有区别的。虽然它们的功能都是通过 Internet 实现邮件通信，但它们采用不同的协议，使用不同的服务器，在功能上也有一些区别。SMTP 邮件服务器接收来自任意发送方的信息，而 POP 服务器只有在用户输入正确的身份信息后才允许对邮箱进行存取。计算机通信通常是一个用户对另一个用户或者一个用户对多个用户，由两个分别称为客户机和服务器之间的交互实现的。电子邮件系统也遵从客户机/服务器结构，即两个程序相配合，将电子邮件从发送人的计算机传送到收信人的邮箱。当用户发送电子邮件时，发信方的计算机就成为一个客户机，收信人的计算机就成为服务器。

当用户结束电子邮件的编辑，客户软件就自动启动。客户软件使用电子邮件的地址来确定与哪一台计算机联系。当服务器接收到电子邮件时，就将它存放到收信人的信箱中。

另外，系统管理员可以建立一个公共信件发送清单，它允许连接到 Internet 上的一个计算机用户向一组收信人发送信件。

6.11.1.4 超文本传输协议

1. WWW 的工作原理

WWW 是基于客户机/服务器模式的应用系统。WWW 服务器负责对各种信息进行组织，WWW 客户机(浏览器)负责如何显示信息和向服务器发送请求。客户机和服务器之间的传输协议采用的是超文本传输协议(HTTP)。服务器端软件通常称为 WWW 服务器，客户端软件通常称为浏览器。

2. URL

要在全网范围内确定一个页，网页名称必须包括以下 3 个部分：页的存放地址、页在宿主机中的全路径名和页的访问方法。符合这种条件的名字称为统一资源定位器(Uniform Resource Locator，URL)。URL 通常用以下形式表示：

<协议类型>://<主机地址>[:端口号]/[<文件路径>]

3. 超文本传输协议(HTTP)

HTTP 采用了客户机/服务器模式，在服务器与客户机之间建立一条 TCP 连接。默认情况下，服务器使用熟知端口 80，而客户机使用短暂端口。

HTTP 是一种面向事务的应用层协议，每一事务的处理是独立的。通常情况下，HTTP 会为每一事务创建一个客户机与服务器间的 TCP 连接，一旦事务处理结束，HTTP 就切断客户机与服务器间的连接，若客户机取下一个文件时，还要重新建立连接。

HTTP 将一次请求/服务的全过程定义为一个简单事务处理，它由以下 4 个步骤组成。

(1) 客户机与服务器建立连接。

(2) 客户机向服务器提出请求，在请求中指明欲操作的页。

(3) 如果请求被接受，服务器送回应答。

(4) 客户机与服务器断开连接。

HTTP 报文有以下两种：请求报文和响应报文。它们都由 3 个部分组成：开始行(用于区分是请求报文还是响应报文)、首部行(说明浏览器、服务器或报文主体的一些信息)和实体主体(报文中的内容)。

4. HTML

HTML(超文本标记语言)是制作网页的语言。HTML 中的命令称为标记(tag)，标记的语法格式如下：

<tag>信息</tag>

例如，<HEAD>和</HEAD>分别表示网页头部的开始和结束，而<BODY>和</BODY>则分别表示网页主体的开始和结束。

6.11.1.5　P2P 应用

1. P2P 的概念

P2P 即对等网络，也就是对等计算机网络，是一种在对等者(Peer)之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。“Peer”在英语里有“对等者”“伙伴”“对端”的意义。因此，从字面上，P2P 可以理解为对等计算或对等网络。国内一些媒体将 P2P 翻译成“点对点”或者“端对端”，学术界则统一称为对等网络(Peer-to-peer networking)或对等计算(Peer-to-peer computing)，其可以定义为：网络的参与者共享他们所拥有的一部分硬件资源(处理能力、存储能力、网络连接能力、打印机等)，这些共享资源通过网络提供服务和内容，能被其他对等节点(Peer)直接访问而无须经过中间实体。在此网络中的参与者既是资源、服务和内容的提供者(Server)，又是资源、服务和内容的获取者(Client)。

在 P2P 网络环境中，彼此连接的多台计算机之间都处于对等的地位，各台计算机有相同的功能，无主从之分，一台计算机既可作为服务器，设定共享资源供网络中其他计算机所使用，又可以作为工作站，整个网络一般来说不依赖专用的集中服务器，也没有专用的工作站。网络中的每一台计算机既能充当网络服务的请求者，又对其他计算机的请求做出响应，提供资源、服务和内容。通常这些资源和服务包括：信息的共享和交换、计算资源(如

CPU计算能力共享)、存储共享(如缓存和磁盘空间的使用)、网络共享、打印机共享等。

2. P2P技术的特点

P2P网络技术的特点体现在以下几个方面。

(1) 非中心化：网络中的资源和服务分散在所有节点上，信息的传输和服务的实现都直接在节点之间进行，可以无须中间环节和服务器的介入，避免了可能的瓶颈。P2P的非中心化基本特点，带来了其在可扩展性、健壮性等方面的优势。

(2) 可扩展性：在P2P网络中，随着用户的加入，不仅服务的需求增加了，系统整体的资源和服务能力也在同步地扩充，始终能比较容易地满足用户的需要。理论上其可扩展性几乎可以认为是无限的。例如：在传统的通过FTP的文件下载方式中，当下载用户增加之后，下载速度会变得越来越慢；然而P2P网络正好相反，加入的用户越多，P2P网络中提供的资源就越多，下载的速度反而越快。

(3) 健壮性：P2P架构天生具有耐攻击、高容错的优点。由于服务是分散在各个节点之间进行的，部分节点或网络遭到破坏对其他部分的影响很小。P2P网络一般在部分节点失效时能够自动调整整体拓扑，保持其他节点的连通性。P2P网络通常都是以自组织的方式建立起来的，并允许节点自由地加入和离开。

(4) 高性价比：性能优势是P2P被广泛关注的一个重要原因。随着硬件技术的发展，个人计算机的计算和存储能力以及网络带宽等性能依照摩尔定理高速增长。采用P2P架构可以有效地利用互联网中散布的大量普通节点，将计算任务或存储资料分布到所有节点上。利用其中闲置的计算能力或存储空间，达到高性能计算和海量存储的目的。目前，P2P在这方面的应用多在学术研究方面，一旦技术成熟，能够在工业领域推广，则可以为许多企业节省购买大型服务器的成本。

(5) 隐私保护：在P2P网络中，由于信息的传输分散在各节点之间进行而无须经过某个集中环节，用户的隐私信息被窃听和泄露的可能性大大缩小。此外，目前解决Internet隐私问题主要采用中继转发的技术方法，从而将通信的参与者隐藏在众多的网络实体之中。在传统的一些匿名通信系统中，实现这一机制依赖于某些中继服务器节点。而在P2P中，所有参与者都可以提供中继转发的功能，因而大大提高了匿名通信的灵活性和可靠性，能够为用户提供更好的隐私保护。

(6) 负载均衡：P2P网络环境下由于每个节点既是服务器又是客户机，减少了对传统C/S结构服务器计算能力、存储能力的要求，同时因为资源分布在多个节点，更好地实现了整个网络的负载均衡。

3. P2P的应用

目前，P2P网络计算技术正不断应用到军事、商业、政务、电信、通信等领域。根据具体应用不同，可以把P2P应用大致分为以下类型。

(1) 文件内容共享和下载，例如Napster、Gnutella、eDonkey、eMule、Maze、BT等，用户可以直接从任意一台安装同类软件的PC上下载或上传文件，并检索、复制共享的文件。

(2) 计算能力和存储共享，例如SETI@home、Avaki、Popular Power、Netbatch、Farsite等，可用于在网络上将存储对象分散存储，或利用其空闲时间进行协同计算。

(3) 基于P2P技术的协同处理与服务共享平台，例如JXTA、Magi、Groove等，可用

于企业管理。

(4) 即时通信工具，包括 ICQ、QQ、Yahoo Messenger、MSN Messenger 等，多个用户可以通过文字、语音或文件进行交流，甚至还可以与手机通信。

(5) P2P 通信与信息共享，例如 Skype、Crowds、Onion Routing 等。

(6) 基于 P2P 技术的网络电视和网络游戏，如沸点、PPStream、PPLive、QQLive、SopCast 等，当前许多网络游戏也是通过对等网络方式实现的。

6.11.2　典型例题分析

例 6-64　在一台服务器上只开放 25 和 110 两个端口，这台服务器可以提供__(39)__服务。(2017 年下半年真题 39)

A. E-mail　　B. Web　　C. DNS　　D. FTP

解析：端口 25 对应的是 SMTP 协议，110 对应的是 POP3 协议，一个是发邮件的协议，一个是读取邮件的协议，因此这是一台邮件服务器。

答案：A

例 6-65　POP3 服务器默认使用__(36)__的__(37)__端口。(2016 年下半年真题 36、37)

(36) A. UDP　　B. TCP　　C. SMTP　　D. HTTP

(37) A. 21　　B. 25　　C. 53　　D. 110

解析：客户机通过 POP3 协议接收邮件，POP3 传输层基于 TCP 协议，端口号是 110。

答案：(36) B　(37) D

例 6-66　当接收邮件时，客户端与 POP3 服务器之间通过__(39)__建立连接，所使用的端口是__(40)__。(2016 年上半年真题 39、40)

(39) A. UDP　　B. TCP　　C. HTTP　　D. HTTPS

(40) A. 25　　B. 52　　C. 1100　　D. 110

解析：POP3 协议的默认端口：110;

POP3 默认传输协议：TCP;

POP3 适用的构架结构：C/S;

POP3 的访问模式：离线访问。

答案：(39) B　(40) D

例 6-67　POP3 协议采用__(28)__模式，客户端代理与 POP3 服务器通过建立__(29)__连接来传送数据。(2015 年下半年真题 28、29)

(28) A. Browser/Server　　B. Client/Server

C. Peer to Peer　　D. Peer to Server

(29) A. TCP　　B. UDP　　C. P2P　　D. IP

解析：电子邮件过程：发件人调用 PC 机中的用户代理撰写和编辑要发送的邮件。发件人的用户代理把邮件用 SMTP 协议发给发送方邮件服务器，SMTP 服务器把邮件临时存放在邮件缓存队列中，等待发送。发送方邮件服务器的 SMTP 客户机与接收方邮件服务器的 SMTP 服务器建立 TCP 连接，然后就把邮件缓存队列中的邮件依次发送出去。运行在接收方邮件服务器中的 SMTP 服务器进程收到邮件后，把邮件放入收件人的用户邮箱中，等待收件人进行读取。收件人在打算收信时，就运行 PC 机中的用户代理，使用 POP3(或

IMAP)协议读取发送给自己的邮件。注意，POP3 服务器和 POP3 客户机之间的通信是由 POP3 客户机发起的。其中 SMTP 和 POP3 协议的传输层的承载协议都是 TCP。

答案：(28) B (29) A

例 6-68 有较高实时性要求的应用是__(28)__。(2015 年上半年真题 28)

A. 电子邮件 B. 网页浏览 C. VoIP D. 网络管理

解析：VoIP 即网络电话，将模拟的声音信号经过压缩与封包之后，以数据包的形式在 IP 网络中进行语音信号的传输，通俗来说也就是互联网电话或 IP 电话。显然，VoIP 对实时性的要求较高。

答案：C

6.11.3 同步练习

1. FTP 客户上传文件时，通过服务器建立的连接是__(1)__，FTP 客户端应用进程的端口可以为__(2)__。

(1) A. 建立在 TCP 之上的控制连接 B. 建立在 TCP 之上的数据连接
C. 建立在 UDP 之上的控制连接 D. 建立在 UCP 之上的数据连接

(2) A. 20 B. 21 C. 80 D. 4155

2. POP3 协议采用__(1)__模式，当客户机需要服务时，客户端软件(Outlook Express 或 Fox Mail)与 POP3 服务器建立__(2)__连接。

(1) A. Browser/Server B. Client/Server C. Peer to Peer D. Peer to Server

(2) A. TCP B. UDP C. PHP D. IP

3. SMTP 服务器端使用的端口号默认为______。

A. 21 B. 25 C. 53 D. 80

4. Telnet 采用客户机/服务器工作方式，采用______格式实现客户机和服务器的数据传输。

A. NTL B. NVT C. base-64 D. RFC 822

5. ftp 命令中用来设置客户端当前工作目录的命令是______。

A. get B. list C. lcd D. !list

6. HTTP 协议中，用于读取一个网页的操作方法为______。

A. READ B. GET C. HEAD D. POST

7. 若 FTP 服务器开启了匿名访问功能，匿名登录时需要输入的用户名是____。

A. root B. user C. guest D. anonymous

8. 使用______协议远程配置交换机。

A. Telnet B. FTP C. HTTP D. PPP

6.11.4 同步练习参考答案

1. (1) B (2) D

2. (1) B (2) A

3. B 4. B 5. C 6. B 7. D 8. A

6.12 本章小结

本章知识点在 2009 年的新大纲中将 IPv6 相关内容分离了出去。

本章主要介绍了网络互联技术和互联网的应用，Internet 服务、域名、IP 地址，包括 IPv4 和 IPv6 地址及其分配。

本章相关知识点在历次考试中分布相对集中，分值在 9 分左右，是考试的重点。根据往年的考题，本章的内容比较多，而且在往年的考题中曾多次出现，所以要以典型例题为主线，抓住重点。本章每节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

6.13 达标训练题及参考答案

6.13.1 达标训练题

1. 各种联网设备的功能不同，路由器的主要功能是________。

A. 根据路由表进行分组转发　　B. 负责网络访问层的安全

C. 分配 VLAN 成员　　D. 扩大局域网覆盖范围

2. 关于网桥和交换机，下面的描述中正确的是________。

A. 网桥端口数少，因而比交换机转发得更快

B. 网桥转发广播帧，而交换机不转发广播帧

C. 交换机是一种多端口网桥

D. 交换机端口多，因而扩大了冲突域的大小

3. 如果指定子网掩码为 256.256.254.0，则________地址可以被赋予一个主机。

A. 112.10.4.0　　B. 186.56.3.0　　C. 117.30.3.255　　D. 17.34.36.0

4. 某个网络中包含 320 台主机，采用子网掩码________可以把这些主机置于同一个子网中而且不浪费地址。

A. 256.256.256.0　　B. 256.256.254.0

C. 256.256.252.0　　D. 256.256.248.0

5. 如果 DHCP 服务器分配的默认网关地址是 192.168.6.33/28，则主机的有效地址应该是________。

A. 192.168.6.55　　B. 192.168.6.47

C. 192.168.6.10　　D. 192.168.6.32

6. 下面的地址中________可以用于公共互联网中。

A. 10.172.12.56　　B. 172.64.12.23

C. 192.168.22.78　　D. 172.16.33.124

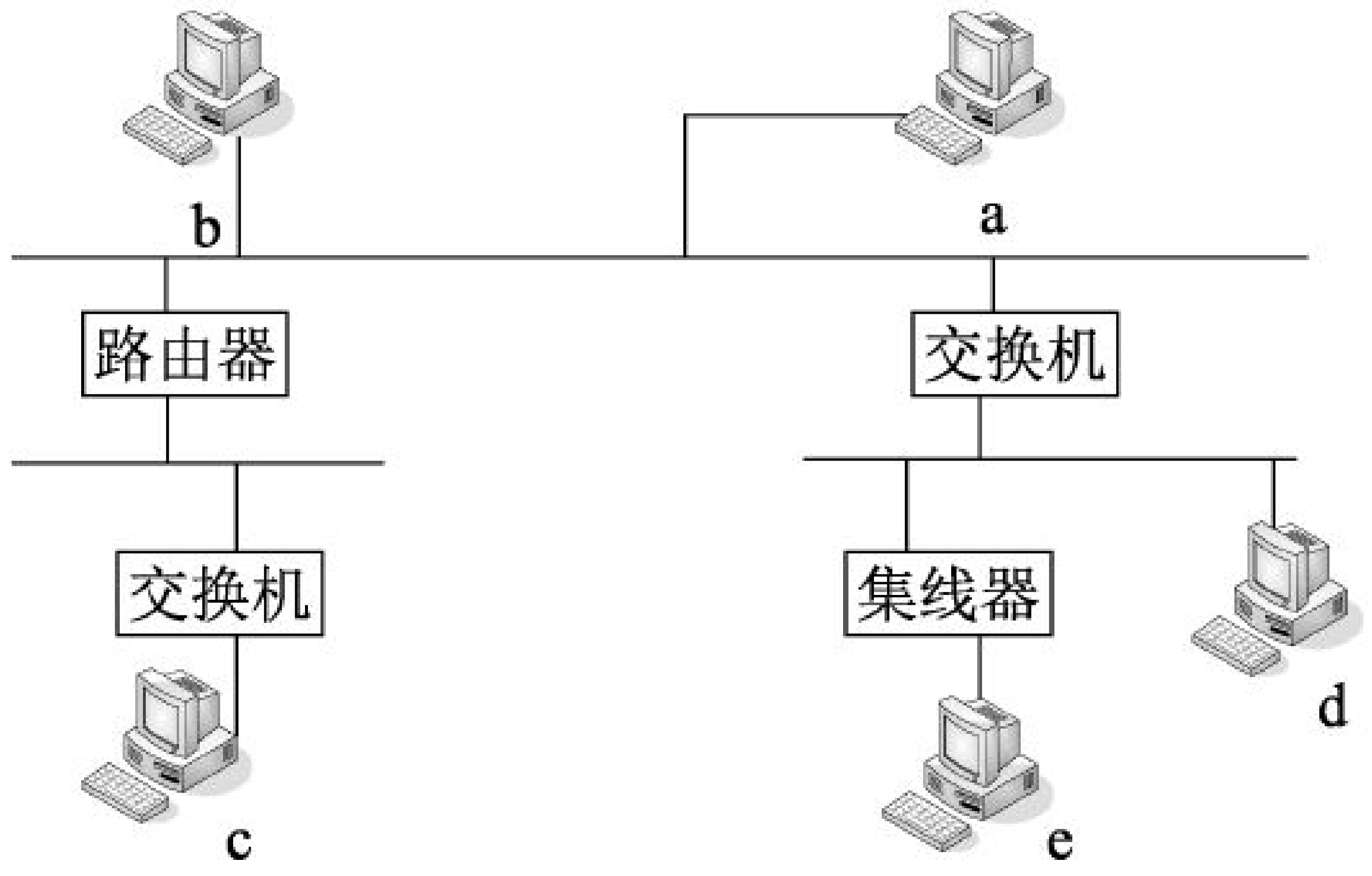
7. 一家连锁店需要设计一种编址方案来支持全国各个门店销售网络，门店有 300 家

左右，每个门店有一个子网，每个子网中的终端最多有 50 台，该连锁店从 ISP 处得到一个 B 类地址，应该采用的子网掩码是________。

A. 256.256.256.128　　B. 256.256.252.0

C. 256.256.248.0　　D. 256.256.256.224

8. 下面的地址中，属于全局广播地址的是__(1)__。在下面的网络中，IP 全局广播分组不能通过的通路是__(2)__。



(1) A. 172.17.256.255　　B. 0.256.256.255

C. 256.256.256.255　　D. 10.256.256.255

(2) A. a 和 b 之间的通路　　B. a 和 c 之间的通路

C. b 和 d 之间的通路　　D. b 和 e 之间的通路

9. 下面的 D 类地址中，可用于本地子网作为组播地址分配的是__(1)__，一个多播组包含 4 个成员，当组播服务发送信息时需要发出__(2)__个分组。

(1) A. 224.0.0.1　　B. 224.0.1.1　　C. 234.0.0.1　　D. 239.0.1.1

(2) A. 1　　B. 2　　C. 3　　D. 4

10. 把网络 10.1.0.0/16 进一步划分为子网 10.1.0.0/18，则原网络被划分为______个子网。

A. 2　　B. 3　　C. 4　　D. 6

11. IP 地址 202.117.17.255/22 是什么地址？______

A. 网络地址　　B. 全局广播地址

C. 主机地址　　D. 定向广播地址

12. IP 地址分为公网地址和私网地址，以下地址中属于私网地址的是______。

A. 10.216.33.124　　B. 127.0.0.1

C. 172.34.21.15　　D. 192.32.146.23

13. 如果子网 172.6.32.0/20 被划分为子网 172.6.32.0/26，则下面的结论中正确的是______。

A. 被划分为 62 个子网　　B. 每个子网有 64 个主机地址

C. 被划分为 32 个子网　　D. 每个子网有 62 个主机地址

14. 地址 192.168.37.192/25 是__(1)__，地址 172.17.17.255/23 是__(2)__。

(1)、(2) A. 网络地址　　B. 组播地址

C. 主机地址　　D. 定向广播地址

15. 某公司有 2000 台主机，则必须给它分配__(1)__个 C 类网络。为了使该公司的网络

地址在路由表中只占一行，给它指定的子网掩码必须是__(2)__。

(1)　A. 2　　B. 8　　C. 16　　D. 24

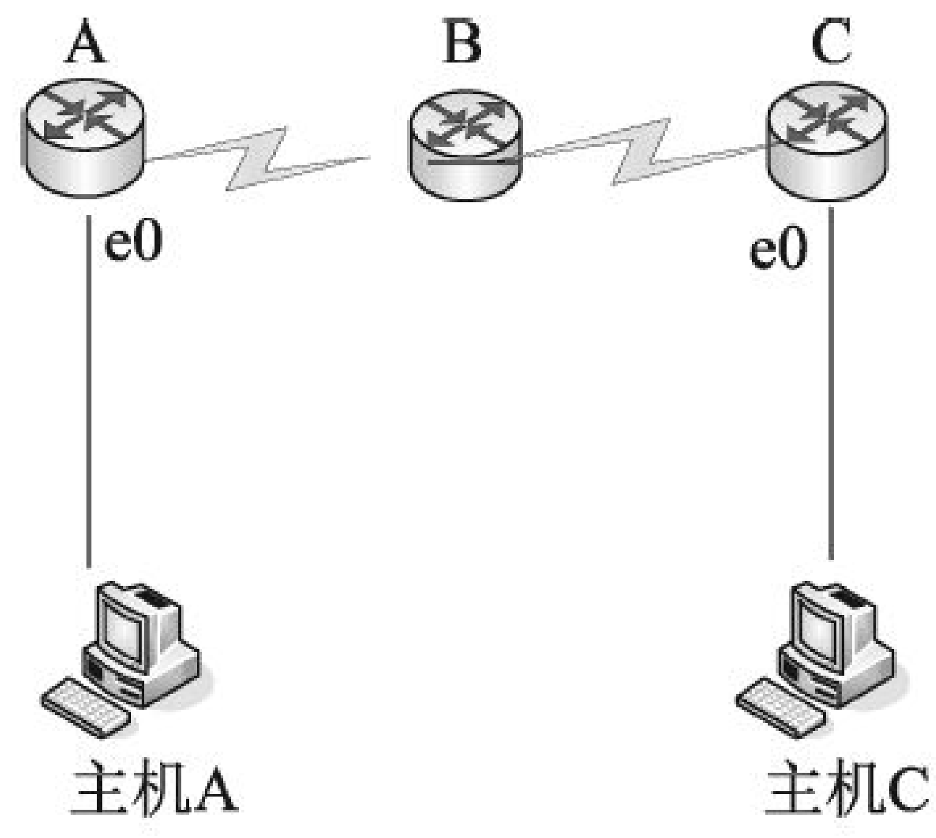
(2)　A. 256.192.0.0　　B. 256.240.0.0　　C. 256.256.240.0　　D. 256.256.248.0

16. 以下给出的地址中，属于子网 172.112.16.19/28 的主机地址是______。

A. 172.112.16.17　　B. 172.112.16.14

C. 172.112.16.16　　D. 172.112.16.31

17. 如下图所示，若路由器 C 的 e0 端口状态为 down，则当主机 A 向主机 C 发送数据时，路由器 C 发送________。



A. ICMP 回声请求报文　　B. ICMP 参数问题报文

C. ICMP 目标不可到达报文　　D. ICMP 源控制报文

18. 以下关于 ICMP 的说法中，正确的是______。

A. 由 MAC 地址求对应的 IP 地址

B. 在公网 IP 地址与私网 IP 地址之间进行转换

C. 向源主机发送传输错误警告

D. 向主机分配动态 IP 地址

19. ICMP 的功能包括__(1)__。当网络通信出现拥塞时，路由器发出 ICMP__(2)__报文。

(1)　A. 传递路由信息　　B. 报告通信故障

C. 分配网络地址　　D. 管理用户连接

(2)　A. 回声请求　　B. 掩码请求

C. 源抑制　　D. 路由重定向

20. 在 TCP/IP 分层结构中，SNMP 是在________之上的异步/请求响应。

A. TCP　　B. UDP　　C. HTTP　　D. P2P

21. 下面________字段的信息出现在 TCP 头部而不出现在 UDP 头部。

A. 目标端口号　　B. 顺序号

C. 源端口号　　D. 校验和

22. 当一个 TCP 连接处于________状态时等待应用程序关闭端口。

A. CLOSED　　B. ESTABLISHED

C. CLOSE-WAIT　　D. LAST-ACK

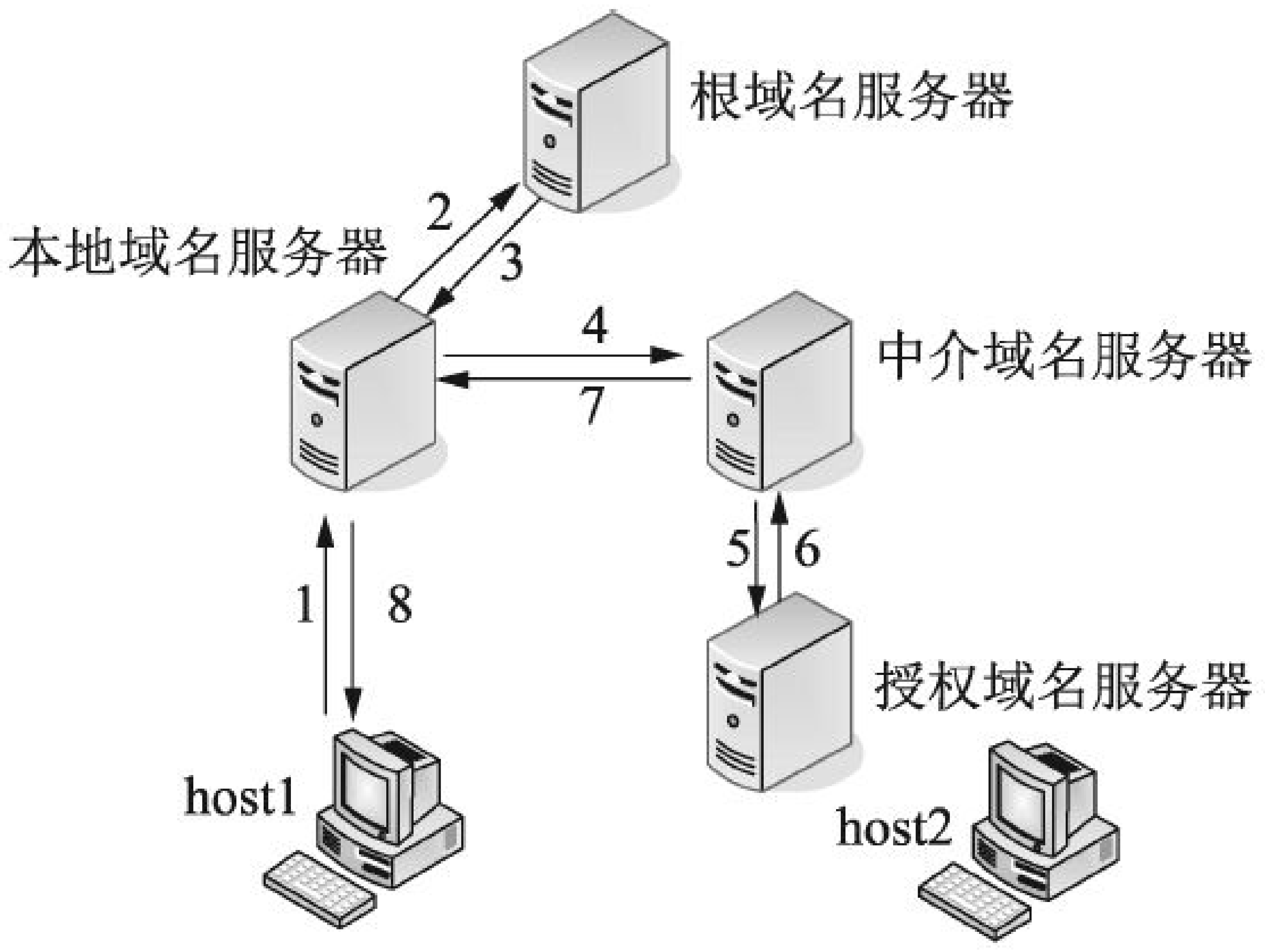
23. TCP 使用__(1)__次握手机制建立连接，当请求方发出 SYN 连接请求后，等待对方回答__(2)__，这样可以防止建立错误的连接。

(1)　A. 1　　B. 2　　C. 3　　D. 4

(2) A. SYN，ACK　　B. FIN，ACK
C. PSH，ACK　　D. RST，ACK

24. 当一个主机要获取通信目标的 MAC 地址时，________。
A. 单播 ARP 请求到默认网关　　B. 广播发送 ARP 请求
C. 与对方主机建立 TCP 连接　　D. 转发 IP 数据报到邻居节点

25. 主机 host 1 和 host 2 进行域名查询的过程如下图所示，下列说法中正确的是________。



A. 根域名服务器采用迭代查询，中介域名服务器采用递归查询
B. 根域名服务器采用递归查询，中介域名服务器采用迭代查询
C. 根域名服务器和中介域名服务器均采用迭代查询
D. 根域名服务器和中介域名服务器均采用递归查询

26. 以下关于 RARP 协议的说法中，正确的是______。
A. RARP 协议根据主机 IP 地址查询对应的 MAC 地址
B. RARP 协议用于对 IP 进行差错控制
C. RARP 协议根据 MAC 地址求主机对应的 IP 地址
D. RARP 协议根据交换的路由信息动态改变路由表

27. “代理 ARP”是指由______假装目标主机回答源主机的 ARP 请求。
A. 离源主机最近的交换机　　B. 离源主机最近的路由器
C. 离目标主机最近的交换机　　D. 离目标主机最近的路由器

28. ARP 协议的作用是__(1)__，它的协议数据单元封装在__(2)__中传送。ARP 请求是采用__(3)__方式发送的。
(1) A. 由 MAC 地址求 IP 地址　　B. 由 IP 地址求 MAC 地址
C. 由 IP 地址查域名　　D. 由域名查 IP 地址
(2) A. IP 分组　　B. 以太帧　　C. TCP 段　　D. UDP 报文
(3) A. 单播　　B. 组播　　C. 广播　　D. 点播

29. 下列描述中，不属于链路状态路由协议的特点的是________。
A. 提供了整个网络的拓扑视图　　B. 计算到达各个目标的最短通路
C. 邻居节点之间互相交换路由表　　D. 具有事件触发的路由更新功能

30. OSPF 网络可以划分成多个区域(area)，下面对于区域的描述中错误的是________。(2013 年年上半年真题)

A. 区域可以被赋予 0～65 535 中的任何编号
B. 单域 OSPF 网络必须配置为区域 1
C. 区域 0 被称为主干网
D. 分层的 OSPF 网络必须划分为多个区域

31. 与 RIPv1 相比，RIPv2 的改进是________。

A. 采用了可变长子网掩码　　B. 使用 SPF 算法计算最短路由
C. 广播发布路由更新信息　　D. 采用了更复杂的路由度量算法

32. 在 BGP4 中，__(1)__报文建立两个路由器之间的邻居关系，__(2)__报文给出了新的路由信息。

(1)、(2) A. 打开(Open)　　B. 更新(Update)
C. 保持活动(Keepallive)　　D. 通告(Notification)

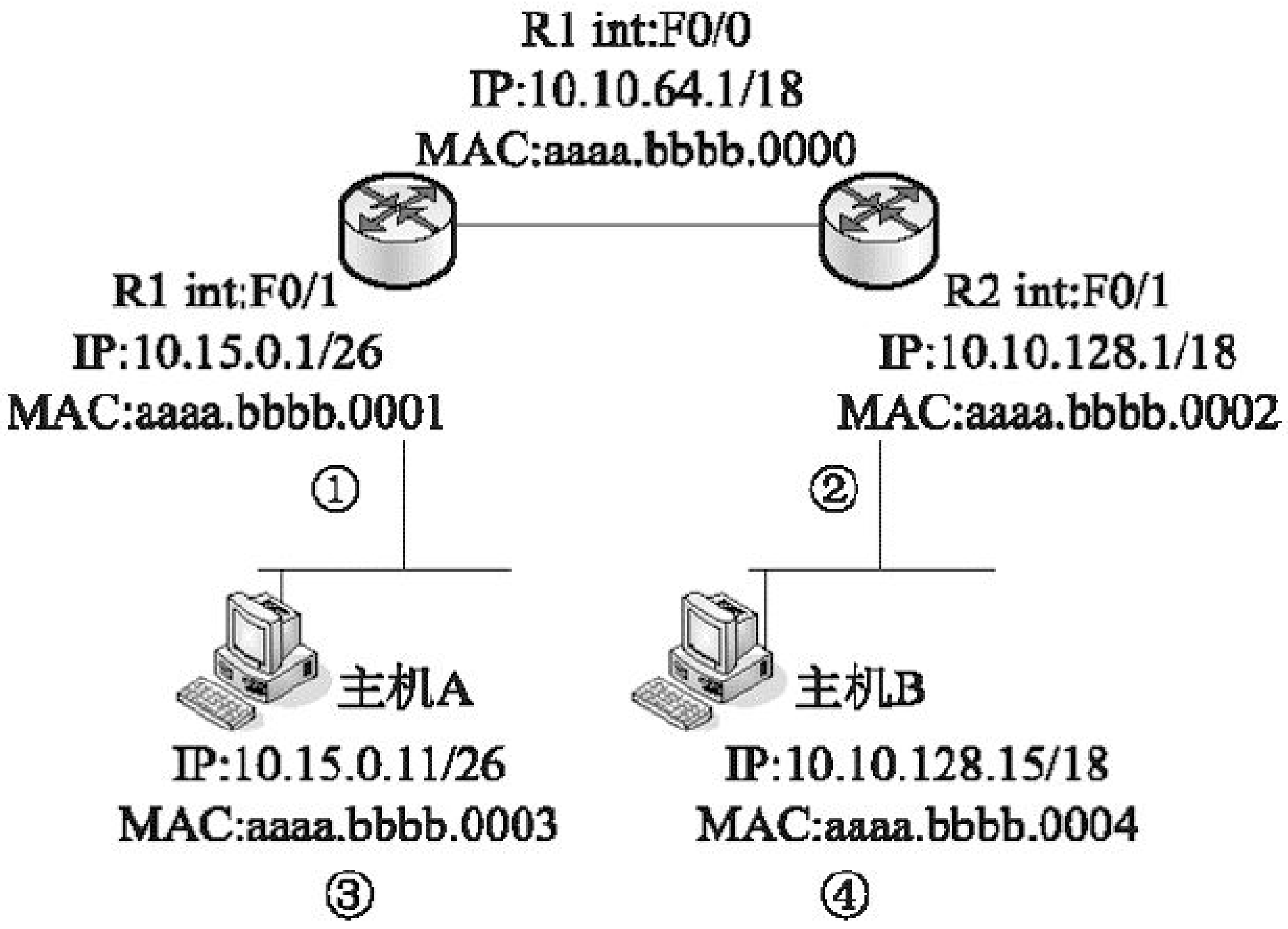
33. 在 OSPF 协议中，链路状态算法用于______。

A. 生成链路状态数据库　　B. 计算路由表
C. 产生链路状态公告　　D. 计算发送路由信息的组播树

34. 在距离矢量路由协议中，每一个路由器接收的路由信息来源于______。

A. 网络中的每一个路由器　　B. 它的邻居路由器
C. 主机中存储的一个路由总表　　D. 距离不超过两个跳步的其他路由器

35. 参见下图，主机 A ping 主机 B，当数据帧到达主机 B 时，其中包含的源 MAC 地址和源 IP 地址为________。



A. aaaa.bbbb.0003 和 10.16.0.11　　B. aaaa.bbbb.0002 和 10.10.128.1
C. aaaa.bbbb.0002 和 10.16.0.11　　D. aaaa.bbbb.0000 和 10.10.64.1

36. 把网络 117.16.32.0/23 划分为 117.16.32.0/27，则得到的子网是__(1)__个，每个子网中可使用的主机地址是__(2)__个。

(1) A. 4　　B. 8　　C. 16　　D. 32
(2) A. 30　　B. 31　　C. 32　　D. 34

37. 4 条路由：124.23.129.0/24、124.23.130.0/24、124.23.132.0/24 和 124.23.133.0/24 经

过汇聚后得到的网络地址是________。

A. 124.23.128.0/21　　B. 124.23.128.0/22

C. 124.23.130.0/22　　D. 124.23.132.0/23

38. 下面的 IP 地址中________属于 CIDR 地址块 120.64.4.0/22。

A. 120.64.8.32　　B. 120.64.7.64

C. 120.64.12.128　　D. 120.64.3.255

39. 有一种 NAT 技术叫作“地址伪装(Masquerading)”，下面的关于地址伪装的描述中正确的是______。

A. 把多个内部地址翻译成一个外部地址和多个端口号

B. 把多个外部地址翻译成一个内部地址和一个端口号

C. 把一个内部地址翻译成多个外部地址和多个端口号

D. 把一个外部地址翻译成多个内部地址和一个端口号

40. 对下面 4 条路由：202.116.129.0/24、202.116.130.0/24、202.116.132.0/24 和 202.116.133.0/24 进行路由汇聚，能覆盖这 4 条路由的地址是______。

A. 202.116.128.0/21　　B. 202.116.128.0/22

C. 202.116.130.0/22　　D. 202.116.132.0/23

41. 可以用于表示地址块 220.17.0.0～220.17.7.0 的网络地址是__(1)__，这个地址块中可以分配__(2)__个主机地址。

(1) A. 220.17.0.0/20　　B. 220.17.0.0/21

C. 220.17.0.0/16　　D. 220.17.0.0/24

(2) A. 2032　　B. 2048　　C. 2000　　D. 2056

42. 网络中存在各种交换设备，下面的说法中错误的是______。

A. 以太网交换机根据 MAC 地址进行交换

B. 帧中继交换机只能根据虚电路号(DLCI)进行交换

C. 3 层交换机只能根据第三层协议进行交换

D. ATM 交换机根据虚电路标识进行信元交换

43. 下列不属于电子邮件协议的是______。

A. POP3　　B. SMTP　　C. SNMP　　D. IMAP4

44. FTP 默认的控制连接端口是______。

A. 20　　B. 21　　C. 23　　D.25

45. 客户端登录 FTP 服务器后使用______命令来上传文件。

A. get　　B. !dir　　C. put　　D. bye

6.13.2 参考答案

1. A	2. B	3. B	4. B
5. C	6. B	7. A	8. (1) C (2) B
9. (1) D (2) A	10. C	11. C	12. A
13. D	14. (1) C (2) D		15. (1) B (2) D

16. A　17. C　18. C　19. (1) B　(2) C
20. B　21. B　22. C　23. (1) C　(2) A
24. B　25. A　26. C　27. B
28. (1) B　(2) B　(3) C　29. C　30. B　31. A
32. (1) A　(2) B　33. B　34. B　35. C
36. (1) C　(2) A　37. A　38. B　39. A
40. A　41. (1) B　(2) A　42.C　43. C
44. B　45. C

第 7 章　下一代互联网

大纲要求：

- IPv6：IPv6 分组格式、IPv6 前地址格式前缀、IPv6 地址分类、IPv6 协议。
- 移动 IP：移动 IP 的通信过程，移动 IPv6 的工作机制。
- 从 IPv4 向 IPv6 的过渡：隧道技术、双协议栈技术、翻译技术。

7.1　IPv6

7.1.1　考点辅导

1. IPv4 的局限性

IPv4 的局限性主要表现在：32 位的 IP 地址空间将无法满足因特网迅速增长的要求；不定长的数据报头域处理影响了路由器的性能提高；单调的服务类型处理；缺乏安全性要求的考虑；负载的分段/组装功能影响了路由器处理的效率。

2. IPv6 的主要特点

IPv6 的主要特点如下。

- 地址长度为 128 位，以支持大规模数量的网络节点。
- IPv6 简化了报头，减少了路由表长度，同时减少了路由器处理报头的时间，降低了报文通过因特网的延迟。
- 增强了选项和扩展功能，使 IPv6 具有更大的灵活性和更强的功能。
- IPv6 对服务质量(QoS)作了定义，IPv6 报文可以标记数据所属的流类型，以便路由器或交换机进行相应的处理。
- IPv6 提供了比 IPv4 更好的安全性保证。

3. IPv6 的表示

IPv6 的地址空间采用 128 位地址长度，几乎可以不受限制地提供地址。

1)　IPv6 地址的表示

IPv6 地址的长度为 128 位，使用冒号分开的十六进制数来表示，例如 21DA:0000:0000:0000:00C2: 0EF0:A57E。

某些 IPv6 地址中可能包含一长串 0。当出现这种情况时，可将连续的 0 压缩，例如上述地址可缩写为 21DA:0:0:0:C2:EF0:A57E；如果有多个连续的 0000，可用双冒号来代替，例如上述地址可进一步缩写成 21DA::C2:EF0:A57E。

2)　IPv6 计算机中 IPv4 地址的表示

IPv6 计算机中 IPv4 地址的表示有两种格式：兼容的和映射的。

- 兼容地址：96 位 0 和 32 位的 IPv4 地址，用于 IPv6 计算机要将报文发送给另一个 IPv6 计算机，但需要通过 IPv4 的区域。例如，IPv4 地址 2.13.17.14 的兼容的 IPv6 地址是 0::020D:110E。
- 映射地址：80 位的 0 后面跟着 16 位的 1，再接 32 位的 IPv4 地址，用于 IPv6 计算机给 IPv4 计算机发送报文。例如，IPv4 地址 2.13.17.14 映射的 IPv6 地址是 0::FFFF:020D:110E。

3) IPv6 地址的分类

IPv6 地址有 3 种基本类型：单播地址、多播地址和任播地址。其中，任播地址是 IPv6 新增的一种地址类型，任播的目的站是一组计算机，但数据包在交付时只交付给其中的一个，通常是距离最近的一个。

4. IPv6 数据包的格式

IPv6 数据包有一个 40 字节的基本首部，其后可允许有零个或多个扩展首部，再后面是数据，如图 7-1 所示。

图 7-1　IPv6 数据报

7.1.2 典型例题分析

例 7-1　以下关于在 IPv6 中任意播地址的叙述中，错误的是__(58)__。(2017 年下半年真题 58)

A. 只能指定给 IPv6 路由器　　B. 可以用作目标地址

C. 可以用作源地址　　D. 代表一组接口的标识符

解析：任意播地址是一个标识符对应多个接口的情况。如果一个数据报文要求被传送到一个任意点地址，则将被传送到最近一个接口(路由器决定)。IPv6 任意播地址只能做目标地址而不能做源地址，也不能指定给 IPv6 主机，而只能指定给 IPv6 路由器。

答案：C

例 7-2　IPv6 链路本地单播地址的前缀为__(60)__，可聚集全球单播地址的前缀为__(61)__ (2017 年上半年真题 60、61)

(60)、(61) A. 001　　B. 1111111010　　C. 1111111011　　D. 11111111

解析：链路本地单播地址的格式前缀为 1111 1110 10，即 FE80::/64，其后是 64 位的接口 ID。IPv6 的可聚集全球单播地址是可以在全球范围内进行路由转发的 IPv6 地址的全球路由选择前缀：分配给各个公司和机构，用于路由器的路由选择。相当于 IPv4 地址中的网络

号，这类地址的前3位是001。

答案：(60) B　(61) A

例 7-3　IPv6 的链路本地地址是在地址前缀 1111 1110 10 之后附加__(18)__形成的。(2016 年下半年真题 18)

A. IPv4 地址　　B. MAC 地址　　C. 主机名　　D. 随机产生的字符串

解析：IPv6 的链路本地地址是在前缀 1111 1110 10 之后附加 MAC 地址形成的，用于同一链路的相邻节点间通信。链路本地地址相当于 IPv4 中的自动专用 IP 地址(APIPA)，可用于邻居发现，并且总是自动配置的。

答案：B

例 7-4　IPv6 地址的格式前缀(FP)用于表示__(60)__。为实现 IP 地址的自动配置，IPv6 主机将__(61)__附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址，如果通过了邻居发现协议的验证，则表明自我配置的链路本地地址是有效的。(2015 年下半年真题 60、61)

(60) A. 地区号　　B. 地址类型或子网地址
C. 网络类型　　D. 播送方式或子网号

(61) A. 32 位二进制随机数　　B. 主机名字
C. 网卡 MAC 地址　　D. IPv4 地址

解析：地址的格式前缀(FP)用于表示地址类型或子网地址，用类似于 IPv4 的 CIDR 表示方法表示。链路本地地址：前缀为 1111 1110 10，用于同一链路的相邻节点间的通信。相当于 IPv4 的自动专用 IP 地址。为实现 IP 地址的自动配置，IPv6 主机将 MAC 地址附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址。

答案：(60) B　(61) C

例 7-5　下面的 4 个 IPv6 地址中，无效地址是__(57)__。(2015 年上半年真题 57)

A. ::192:168:0:1　　B. ::2001:3452:4955:2367::
C. 2002:c0a8:101::43　　D. 2003:dead:beef:4dad:23:34:bb:101

解析：IPv6 地址中一个或多个全 0 字段 0000 可以用一对冒号代替，但不能出现两次代替。

答案：B

7.1.3　同步练习

1.　IPv6 的可聚合全球单播地址前缀为__(1)__，任意播地址的组成是__(2)__。

(1) A. 010　　B. 011　　C. 001　　D. 100

(2) A. 子网前缀＋全 0　　B. 子网前缀＋全 1
C. 链路本地地址前缀＋全 0　　D. 链路本地地址前缀＋全 1

2.　IPv6 地址的格式前缀用于表示地址类型或子网地址。例如 60 位的地址前缀 12AB00000000CD30 有多种合法的表示形式，下面的选项中，不合法的是________。

A. 12AB:0000:0000:CD30:0000:0000:0000:0000/60

B. 12AB::CD30:0:0:0:0/60

C. 12A8:0:0:CD30/60

D. 12AB:0:0:CD30::/60

3. IPv6 新增加了一种任意播地址，这种地址________。

A. 可以用作源地址，也可以用作目标地址

B. 只可以作为源地址，不能作为目标地址

C. 代表一组接口的标识符

D. 可以用作路由器或主机的地址

7.1.4 同步练习参考答案

1. (1) C (2) A 2. C 3. C

7.2 移 动 IP

7.2.1 考点辅导

7.2.1.1 移动 IP 的通信过程

RFC 3344(IPv4 下的移动性支持)给出的解决方案是增强 IPv4 协议，使其能够把 IP 数据报路由到移动主机当前所在的连接站点。按照这个方案，每个移动主机配置了一个家乡地址(home address)作为永久标识。当移动主机离开家乡网络时，通过所在地点的外地代理，它被赋予了一个转交地址(care-of address)。协议提供了一种注册机制，使得移动主机可以通过家乡地址获得转交地地址。家乡代理通过安全隧道可以把分组转发给外地代理，然后被提交给移动主机。

移动 IP 提供了两种获取转交地址的方式。一种是外地代理转交地址(Foreign Agent Care-of Address)，这种转交地址是外地代理在它的代理公告报文中提供的地址，也就是外地代理的 IP 地址。另外一种获取模式是配置转交地址(Collocated Care-of Address)，是暂时分配给移动节点的某个端口的 IP 地址，其网络前缀必须与移动节点当前所连接的外地链路的网络前缀相同。一个配置转交地址只能被一个移动节点使用。可以是通过 DHCP 服务器动态分配的地址，或是在地址缓冲池中选取的私网地址。

7.2.1.2 移动 IPv6

RFC 3775(IPv6 下的移动性支持)规范了 IPv6 对移动主机的支持功能，定义的协议称为移动 IPv6。移动 IPv6 协议既适合于同构型介质，也适合于异构型介质。

1. 移动 IPv6 的工作机制

在移动 IPv6 中，家乡地址是带有移动节点家乡子网前缀的 IP 地址。当移动节点连接在家乡网络中时，发送给家乡地址的分组通过常规的路由机制可以到达移动节点。当移动节点连接到外地链路时，可以通过一个或多个转交地址对其寻址。转交地址是具有外地链路

子网前缀的 IP 地址。移动节点可以通过常规的 IPv6 机制获取转交地址。只要移动节点停留在外部某个位置，发送给转交地址的分组都可以被路由到移动节点。当移动节点处于漫游状态时，它可能从几个转交地址接收分组，只要它还能与以前的链路保持连接。

移动节点与对端节点之间的通信有两种方式。第一种方式是双向隧道，这种情况下不需要移动 IPv6 的支持，即使移动节点没有在对端节点上注册它当前的绑定也可以进行通信。第二种方式是路由优化，要求移动节点把它当前的绑定信息注册到对端节点上，对端节点发出的分组就可以直接路由到移动节点的转交地址。

2. *路由扩展头*

RFC 3775 中定义了一种新的 2 型路由头，其中提供的路由地址只有一个——移动节点的家乡地址，如图 7-2 所示。

下一头部	Hdr Ext Len=2	路由类型=2	未用段=1
保留			
家乡地址			

图 7-2　路由扩展头

3. *移动扩展头*

移动节点、对端节点和家乡代理在生成和管理绑定的过程中都要使用移动头来传输信息。由于为移动头指定的代码是 135，因此在前面的扩展头中要用 135 来指向移动头，如图 7-3 所示。

负载的协议	头长度	MH类型	保留
校验和			
数据报文			

图 7-3　移动扩展头

MH 类型占用一个字节(8 个二进制位)，用于说明报文的类型，具体如下。

- MH=0：绑定刷新请求报文。
- MH=1：家乡测试初始化报文。
- MH=2：转交测试初始化报文。
- MH=3：家乡测试报文。
- MH=4：转交测试报文。
- MH=5：绑定更新报文。
- MH=6：绑定应答报文。
- MH=7：绑定出错报文。

7.2.2　典型例题分析

例 7-6　所谓移动 IP 是指__(58)__，实现移动 IP 的关键技术是__(59)__。(2014 年上半年真题 58、59)

(58) A. 通过地址翻译技术改变主机的 IP 地址
B. 一个主机 IP 地址可以转移给另一个主机
C. 移动主机通过在无线通信网中漫游来保持网络连接
D. 移动主机在离开家乡网络的远程站点可以连接工作站

(59) A. 移动主机具有一个可以接入任何网络的通用 IP 地址
B. 移动主机具有一个家乡网络地址并获取一个外地转交地址
C. 移动主机通过控制全网的管理中心申请网络接入服务
D. 移动主机总是通过家乡网络地址来获取接入服务

解析：移动 IP 是为了满足移动节点在移动中保持其连接性而设计的。移动 IP 现在有两个版本，分别为移动 IPv4(RFC 3344，取代了 RFC 3220、RFC 2002)和移动 IPv6(RFC 3775)。目前广泛使用的仍然是移动 IPv4。

最简单地说，移动 IP 技术就是让计算机在互联网及局域网中不受任何限制地即时漫游，也称移动计算机技术。

专业来说，移动 IP 技术是移动节点(计算机/服务器/网段等)以固定的网络 IP 地址，实现跨越不同网段的漫游功能，并保证了基于网络 IP 的网络权限在漫游过程中不发生任何改变。

移动 IP 的关键技术有代理搜索、转交地址、登录、隧道。

① 代理搜索：是计算节点用来判断自己是否处于漫游状态。
② 转交地址：是移动节点移动到外网时从外网代理处得到的临时地址。
③ 登录：是移动节点到达外网时进行一系列认证、注册、建立隧道的过程。
④ 隧道：是家乡代理与外地代理之间临时建立的双向数据通道。

答案：(58) C　(59) B

7.3　从 IPv4 向 IPv6 的过渡

7.3.1　考点辅导

从 IPv4 向 IPv6 过渡初期要解决的问题可以分成两类：第一类是解决 IPv6 孤岛之间互相通信的问题，第二类是解决 IPv6 孤岛与 IPv4 海洋之间的通信问题。目前提出的过渡技术可以归纳为以下 3 种。

- 隧道技术：用于解决 IPv6 节点之间通过 IPv4 网络进行通信的问题。
- 双协议栈技术：使得 IPv4 和 IPv6 可以共存于同一设备和同一网络中。
- 翻译技术：使得纯 IPv6 节点与纯 IPv4 节点之间可以进行通信。

7.3.1.1 隧道技术

所谓隧道技术，就是把 IPv6 分组封装到 IPv4 分组中，通过 IPv4 网络进行转发的技术。根据隧道端节点的不同，可以分为 4 种不同的隧道：主机到主机的隧道、主机到路由器的隧道、路由器到路由器的隧道、路由器到主机的隧道。

1. 隧道中介技术

隧道中介技术是要求隧道端点必须运行双协议栈，两个端点之间不能使用 NAT 技术，因为 IPv4 地址必须是全局可路由的。对于 IPv4/IPv6 双栈主机，可以配置一条默认的隧道，以便把不能连接到任何 IPv6 路由器的分组发送出去。双栈边界路由器的 IPv4 地址必须是已知的，这是隧道端点的地址。这种默认隧道建立后，所有的 IPv6 目标地址都可以通过隧道传送。

2. 自动隧道

两个双栈主机可以通过自动隧道在 IPv4 网络中进行通信。实现自动隧道的节点必须采用 IPv4 兼容的 IPv6 地址。当分组进入双栈路由器时，如果目标地址是 IPv4 兼容的地址，分组就被重定向，并自动建立一条隧道。如果目标地址是当地的 IPv6 地址，则不会建立自动隧道。被传送的分组决定了隧道的端点，目标 IPv4 地址取自 IPv6 地址的低 32 位，源地址是发送分组的接口的 IPv4 地址。

3. 6to4 隧道

6to4 隧道技术是一种支持 IPv6 站点通过 IPv4 网络进行通信的技术，这种技术不需要显式地建立隧道，可以使得一个原生的 IPv6 站点通过中继路由器连接到 IPv6 网络中。

IANA 在可聚合全球单播地址范围内指定了一个格式前缀 0x2002 来表示 6to4 地址。通常把带有 16 位前缀“2002”的 IPv6 地址称为 6to4 地址，而把不使用这个前缀的 IPv6 地址称为原生地址。

中继路由器是一种经过特别配置的路由器，用于在原生 IPv6 地址与 6to4 地址之间进行转换。6to4 技术都是在边界路由器中实现的，不需要对主机的路由配置做任何改变。6to4 路由器应该配置双协议栈，应该具有全局 IPv4 地址，并能实现 6to4 地址转换。这种方法对 IPv4 路由表不增加任何选项，只是在 IPv6 路由表中引入了一个新的选项。

6to4 路由器应该向本地网络公告它的 6to4 前缀 2002:IPv4::/48，其中，IPv4 是路由器的全局 IPv4 地址。在本地 IPv6 网络中的 6to4 主机要使用这个前缀，可以用作自动的地址赋值，或用作 IPv6 路由，或用在 6over4 机制中。

6to4 技术也支持原生 IPv6 站点到 6to4 站点的通信，还可以支持 6to4 站点到原生 IPv6 站点的通信。

4. 6over4 隧道

RFC 2529 定义的 6over4 是一种由 IPv4 地址生成 IPv6 链路本地地址的方法。IPv4 主机的接口标识符是在该接口的 IPv4 地址前面加 32 个“0”形成的 64 位标识符。IPv6 链路本地地址的格式前缀为 FE80::/64，在其后面加上 64 位的 IPv4 接口标识符就形成了完整的 IPv6 链路本地地址。

RFC 2529 规定，IPv6 组播分组要封装在目标地址为 239.192.x.y 的 IPv4 分组中发送，

其中 x 和 y 是 IPv6 组播地址的最后两个字节。由于 239.192.0.0/16 是 IPv4 机构本地范围内的组播地址块，所以实现 6over4 的主机都要位于同一 IPv4 组播区域内。

IPv6 邻居发现的过程如下：首先是 IPv6 主机组播 ICMPv6 邻居邀请报文，然后是收到对方的邻居公告报文，其中包含了 64 位的链路层地址。当 IPv6 主机获得了对方主机的 IPv4 地址后，就可以用无状态自动配置方式构造源和目标的链路本地地址，向通信对方发送 IPv6 分组了。当然，IPv6 分组还是要封装在 IPv4 分组中传送的。

5. ISATAP

RFC 4214 定义了一种自动隧道技术——ISATAP，ISATAP 意味着通过 IPv4 地址自动生成 IPv6 站点本地地址或链路本地地址，IPv4 地址作为隧道的端点地址，把 IPv6 分组封装在 IPv4 分组中进行传送。

一般来说，ISATAP 地址有 64 位的格式前缀，FEC0::/64 表示站点本地地址，FE80::/64 表示链路本地地址。在格式前缀之后要加上修改的 EUI-64 地址，其形式如下：

24 位的 IANA OUI+40 位的扩展标识符

如果 40 位扩展标识符的前 16 位是 OxFFFE，则后面是 24 位的制造商标识符；如果 40 位扩展标识符的前 8 位是 0xFE，则后面是 32 位的 IPv4 地址。

7.3.1.2　协议翻译技术

已经提出的翻译方法有如下几种。

- SIIT：无状态的 IP/ICMP 翻译。
- NAT-PT：网络地址翻译-协议翻译。
- SOCKS64：基于 SOCKS 的 IPv6/IPv4 机制。
- TRT：IPv6 到 IPv4 的传输中继翻译器。

1. SIIT

SIIT 转换器规范描述了从 IPv6 到 IPv4 的协议转换机制，包括 IP 头的翻译方法以及 ICMP 报文的翻译方法等。当 IPv6 主机发出的分组到达 SIIT 转换器时，IPv6 分组头被翻译为 IPv4 分组头，分组的源地址采用 IPv4 翻译地址，目标地址采用 IPv4 映射地址，然后这个分组就可以在 IPv4 网络中传送了。

IPv4 映射地址：一种内嵌 IPv4 地址的 IPv6 地址，可表示为 0:0:0:0:0:FFFF:w.x.y.z 或::FFFF:w.x.y.z 的形式，其中 w.x.y.z 是 IPv4 地址。这种地址用于仅支持 IPv4 的主机。

IPv4 翻译地址：一种内嵌 IPv4 地址的 IPv6 地址，可表示为 0:0:0:0:FFFF:0:w.x.y.z 或::FFFF:0:w.x.y.z 的形式，其中 w.x.y.z 是 IPv4 地址。这种地址可用于支持 IPv6 的主机。

2. NAT-PT

NAT-PT 是 RFC 2766(网络地址翻译及协议翻译)定义的协议翻译方法。实现 NAT-PT 技术必须指定一个服务器作为 NAT-PT 网关，并且要准备一个 IPv4 地址块作为地址翻译之用，要为每个站点至少预留一个 IPv4 地址。

RFC 2766 定义的是有状态的翻译技术，即要记录和保持会话状态，按照会话状态参数对分组进行翻译，包括对 IP 地址及其相关的字段进行翻译。

NAT-PT 操作有 3 个变种：基本 NAT-PT、NAPT-PT 和双向 NAT-PT。基本 NAT-PT 是

单向的，只允许 IPv6 主机访问 IPv4 主机；NAPT-PT 也是单向通信，但是扩展到了 TCP/UDP 端口的翻译，也包括 ICMP 询问标识符的翻译，这种技术可以实现 IPv6 主机的传输标识符到指定 IPv4 地址传输标识符的多路复用，即让一组 IPv6 主机共享同一 IPv4 地址；双向 NAT-PT，意味着双向通信，无论是 IPv6 主机还是 IPv4 主机，都可以进行翻译。

协议翻译技术适用于 IPv6 孤岛与 IPv4 海洋之间的通信，这种技术要求一次会话中的双向数据包都在同一个路由器上完成转换，所以它只能适用于同一路由器连接的网络。

7.3.1.3 双协议栈技术

双协议栈技术适用于同时实现了 IPv6 和 IPv4 两个协议栈的主机之间进行通信。在这种情况下，当主机发起通信时，DNS 服务器将同时提供 IPv6 和 IPv4 两种地址，主机将根据具体情况使用适当的协议来建立通信。在服务器一边要同时监听 IPv4 和 IPv6 两种端口。

1. BIS

BIS(Bump-In-the-Stack)是应用于 IP 安全域内的一种机制，适用于在开始过渡阶段利用现有的 IPv4 应用进行 IPv6 通信。这种技术是在主机的 TCP/IPv4 模块与网卡驱动模块之间插入一些模块来实现 IPv4 与 IPv6 分组之间的转换，使得主机成为一个协议转换器。

BIS 用 3 个模块来代替 IPv6 应用：转换器、扩展名解析器和地址映射器。转换器的作用是在 IPv4 地址与 IPv6 地址之间进行转换；扩展名解析器对 IPv4 应用发出的请求返回一个“适当的”答案；地址映射器维护一个 IPv4 地址池，同时维护一个由 IPv4 地址与 IPv6 地址对组成的表。

2. BIA

BIA 是在 IPv4 Socket 应用与 IPv6 Socket 应用之间进行翻译的技术。BIA 要求在 Socket 应用模块与 TCP/IP 模块之间插入 API 转换器，这样建立的双栈主机不需要在 IP 头之间进行翻译，使得转换过程得到简化。API 转换器由 3 个模块组成：功能映射器、名字解析器、地址映射器。功能映射器的作用是在 IPv4 Socket API 功能与 IPv6 Socket API 功能之间进行转换。名字解析器的作用是在收到 IPv4 应用请求时给出适当的响应。地址映射器与 BIS 中的地址映射器相同。

7.3.2 典型例题分析

例 7-7 IPv6 站点通过 IPv4 网络通信需要使用隧道技术，常用的 3 种自动隧道技术是 (58) 。(2015 年上半年真题 58)

A. VPN 隧道、PPTP 隧道和 IPsec 隧道

B. 6to4 隧道、6over4 隧道和 ISATAP 隧道

C. VPN 隧道、PPP 隧道和 ISATAP 隧道

D. IPSec 隧道、6over4 隧道和 PPTP 隧道

解析：自动隧道就是隧道接口中的目的地址可以不用配置，直接从 IPv6 地址中提取。自动隧道技术主要有 6to4 隧道技术、6over4 隧道技术和 ISATAP 技术。6to4 隧道技术通过在 IPv6 报文的目的地址中嵌入 IPv4 地址，来实现自动获取隧道终点的 IPv4 地址。6to4 隧

道技术采用特殊的 6to4 地址，其格式为：2002:abcd:efgh:子网号::接口 ID/64，其中 2002 表示固定的 IPv6 地址前缀，abcd:efgh 表示该 6to4 隧道对应的 32 位全球唯一的 IPv4 源地址，用十六进制表示。2002:abcd:efgh 之后的部分唯一标识了一个主机在 6to4 网络内的位置。通过这个嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。6over4 隧道机制是将 IPv6 数据报文前封装上 IPv4 的报文头，通过隧道(Tunnel)使 IPv6 报文穿越 IPv4 网络，实现隔离的 IPv6 网络的互通。SATAP 使用本地管理的接口标识符::0:5EFE:w.x.y.z，其中:: 0: 5EFE 部分是由 Internet 号码分配中心(IANA)所分配的机构单元标识符 (00-00-5E)和表示内嵌的 IPv4 地址类型的类型号(FE)组合而成的。w.x.y.z 部分是任意的单播 IPv4 地址，既可以是私有地址，也可以是公共地址。

答案：B

7.3.3　同步练习

在 IPv4 和 IPv6 混合的网络中，协议翻译技术用于________。

A. 两个 IPv6 主机通过 IPv4 网络通信

B. 两个 IPv4 主机通过 IPv6 网络通信

C. 纯 IPv4 主机和纯 IPv6 主机之间的通信

D. 两个双协议栈主机之间的通信

7.3.4　同步练习参考答案

C

7.4　下一代互联网的发展

推动下一代互联网研究的主要因素有 3 个：一是大幅度地增加 IP 地址供给，二是开发新的网络应用，三是抢占 IT 产业竞争优势。

1. IP 地址的分配

IP 地址和 AS 号码的分配主要由美国掌控。ICANN(the Internet Corporation for Assigned Names and Numbers)是负责互联网国际域名、地址和号码管理的非营利性机构。ICANN 将部分 IP 地址和 AS 号码分配给地区级的互联网注册机构(RIR)，RIR 再将地址分配给区域内的本地互联网注册机构(LIR)和互联网服务提供商(ISP)，然后由他们向用户分配。

现有 5 个 RIR 管理地区：APNIC 是亚太地区互联网络信息中心；ARIN 是美国网络地址注册管理组织，负责北美地区的 IP 地址和 AS 号码的分配；LACNIC 是拉丁美洲及加勒比地区的互联网络信息中心；RIPE NCC 负责欧洲地区 IP 地址和 AS 号码的管理；AfriNIC 是非洲的网络信息中心。

应对 IPv4 地址的耗尽问题已成为全球性的战略问题。2006 年，IANA 已经为五大洲的 RIR 分配了全球单播地址格式前缀。

AfriNIC：2C00:0000::/12

APNIC：2400:0000::/12

ARIN：2600:0000::/12

LACNIC：2800:0000::/12

RIPE NCC：2A00:0000::/12

2. 我国的下一代互联网研究

我国下一代互联网示范工程(CNGI)项目是于 2003 年启动的。截至目前，CNGI 已经建成了由 6 个主干网、两个国际交换中心及相应的传输链路组成的核心网络。6 个主干网是：CERNET2、中国电信、中国网通/中科院、中国移动、中国联通和中国铁通。

1) CERNET2

CERNET2 是 CNGI 中规模最大的主干网，也是目前世界上规模最大的采用纯 IPv6 技术的下一代互联网。它以 2.5～10Gb/s 的速率连接全国 20 个城市的 25 个主干网核心节点。

2) GLORIAD

2004 年 1 月 12 日，中美俄环球科教网络(GLORIAD)正式开通，以支持科研、教育方面的国际合作。GLORIAD 计划包括以下 4 个方面的内容。

(1) 网络传输基础设施的研究和建设。设计传输速率为 10Gb/s。

(2) 网络重要支撑技术的研究、运行和试验。在网络层将采用 IPv6 协议实现互联。

(3) 网络应用服务软件和中间件的研究、运行。采用基于网格的软件技术。

(4) 建立强大的科学教育应用联盟。

7.5 本 章 小 结

本章知识点在 2014 年的新大纲中是从“网络互连与互联网”一章中分离出来的，作为单独的一章，并添加了移动 IP、从 IPv4 向 IPv6 的过渡和下一代互联网的发展等当前主流技术。其中 IPv6 地址是重点，一般考试中都会出现。除此之外，从 IPv4 向 IPv6 的过渡技术也是考核的重点，需要掌握好。

7.6 达标训练题及参考答案

7.6.1 达标训练题

在从 IPv4 向 IPv6 过渡期间，如果要使得两个 IPv6 节点可以通过现有的 IPv4 网络进行通信，则应该使用__(1)__；如果要使得纯 IPv6 节点可以与纯 IPv4 节点进行通信，则需要

使用 __(2)__ 。

(1)、(2) A. 堆栈技术　　B. 双协议栈技术
C. 隧道技术　　D. 翻译技术

7.6.2 参考答案

(1) B　(2) D

第 8 章　网 络 安 全

大纲要求：

- 保密，包括私钥加密体制和公钥加密体制。
- 安全体制，包括认证、数字签名、完整性、访问控制。
- 安全协议。
- 病毒防范和入侵检测。
- 访问控制与防火墙，包括 ACL 命令、过滤规则和防火墙配置。
- 数字证书。
- VPN 配置。
- PGP。

8.1　网络安全的基本概念

8.1.1　考点辅导

8.1.1.1　网络安全威胁的类型

网络安全威胁是对网络安全缺陷的潜在利用。这些缺陷可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏等。网络安全威胁的种类如下。

- 窃听：如搭线窃听、安装通信监视器和读取网上的信息等。
- 假冒：某个实体假装成另一个实体，并获取该实体的权限。
- 重放：重复一份报文或报文的一部分，以便产生一个被授权效果。
- 流量分析：通过对网上信息流的观察和分析推断出网上传输的有用信息。
- 数据完整性破坏：有意或无意地修改或破坏信息系统，或者在非授权和不能检测的方式下对数据进行修改。
- 拒绝服务：通过发送大量的请求来消耗和占用过多的服务资源，使得网络服务不能响应正常的请求。
- 资源的非授权访问：与所定义的安全策略不一致的使用。
- 陷门和特洛伊木马：通过替换系统合法程序，或者在合法程序中插入恶意代码，以实现非授权攻击，从而达到某种特定的目的。
- 病毒：可执行的恶性程序码，通过对其他程序进行修改对计算机数据信息进行破坏，抢占系统资源，影响计算机运行速度。
- 诽谤：散布错误的信息以达到诋毁某个对象的形象和知名度的目的。

8.1.1.2　网络安全漏洞

网络安全隐患主要表现在以下几个方面。

(1)　物理性安全。凡是能够让非授权机器物理接入的地方，都会存在潜在的安全问题。

(2)　软件安全漏洞。

(3)　不兼容使用的安全漏洞。

(4)　选择自认为合适的安全哲理。这是一种对安全概念的理解和直觉。完美的软件、受保护的硬件和兼容部件并不能保证正常而有效地工作，除非用户选择了适当的安全策略和打开了能增加其系统安全的部件。

8.1.1.3　网络攻击

网络攻击是某种安全威胁的具体实现，当信息从信源向信宿流动时，可能受到各种类型的攻击。网络攻击可以分为被动攻击、主动攻击、物理临近攻击、内部人员攻击、分发攻击几类。

1. 被动攻击

被动攻击是对信息的保密性进行攻击，即通过窃听网络上传输的信息并加以分析，从而获得有价值的情报，但它并不修改信息的内容。它的目标是获得正在传送的信息，其特点是偷听或监视信息的传递。主要预防手段是数据加密等。

2. 主动攻击

主动攻击是攻击信息来源的真实性、信息传输的完整性和系统服务的可用性，有意对信息进行修改、插入和删除。主要攻击形式有假冒、重放、欺骗、消息窜改和拒绝服务等。主要预防手段是防火墙、入侵检测技术等。

3. 物理临近攻击

物理临近攻击是指未授权者可在物理上接近网络、系统或设备，其目的是修改、收集或拒绝访问信息。

4. 内部人员攻击

有的内部人员被授权在信息安全处理系统的物理范围内，或对信息安全处理系统具有直接访问权，他们可能会攻击网络。

5. 分发攻击

分发攻击是指在软件和硬件开发出来之后和安装之前这段时间，或者当它从一个地方传到另一个地方时，攻击者恶意修改软硬件。

8.1.1.4　安全措施的目标

安全措施的目标如下。

(1)　访问控制：确保会话对方有权做它所声称的事情。

(2)　认证：确保会话对方的资源同它声称的一致。

(3) 完整性：确保接收到的信息同发送的一致。

(4) 审计：确保任何发生的交易在事后可以被证实，发信者和收信者都认为交换发生过，即不可抵赖性。

(5) 保密：确保敏感信息不被窃听。

8.1.1.5 基本安全技术

目前的网络安全措施有数据加密、数字签名、身份认证、防火墙、入侵检测。

8.1.2 典型例题分析

例 8-1 下列攻击行为中属于典型被动攻击的是 (42) 。(2017 年下半年真题 42)

A. 拒绝服务攻击　　B. 会话拦截　　C. 系统干涉　　D. 修改数据命令

解析：被动攻击是对信息的保密性进行攻击，并不修改信息的内容，其目标是获得正在传送的信息。修改数据命令属于主动攻击。

答案：B

例 8-2 (41) 不属于主动攻击。(2015 年下半年真题 41)

A. 流量分析　　B. 重放　　C. IP 地址欺骗　　D. 拒绝服务

解析：计算机网络上的通信面临以下 4 种威胁。

截获：攻击者从网络上窃听他人的通信内容。

中断：攻击者有意中断他人在网络上的通信。

篡改：攻击者故意篡改网络中传送的报文。

伪造：攻击者伪造信息在网络上传送。

以上 4 种威胁可以划分为两大类，即被动攻击和主动攻击。在上述情况中，截获信息的攻击属于被动攻击，而中断、篡改和伪造信息的攻击称为主动攻击。

答案：A

8.1.3 同步练习

1. 下列不属于主动攻击形式的是________。

   A. 假冒　　B. 欺骗

   C. 消息篡改　　D. 窃听

2. 安全审计是保障计算机系统安全的重要手段，其作用不包括______。

   A. 重现入侵者的操作过程

   B. 发现计算机系统的滥用情况

   C. 根据系统运行的日志，发现潜在的安全漏洞

   D. 保证可信计算机系统内部信息不外泄

8.1.4 同步练习参考答案

1. D　2. D

8.2 信息加密技术

8.2.1 考点辅导

8.2.1.1 数据加密原理

一般的数据加密模型如图 8-1 所示。在发送端，把明文 X 用加密算法 E 和加密密钥 K 加密，变换成密文 Y，即 $Y=E_K(X)$；在接收端利用解密算法 D 和解密密钥 K 对密文 Y 进行解密，得到明文 X。

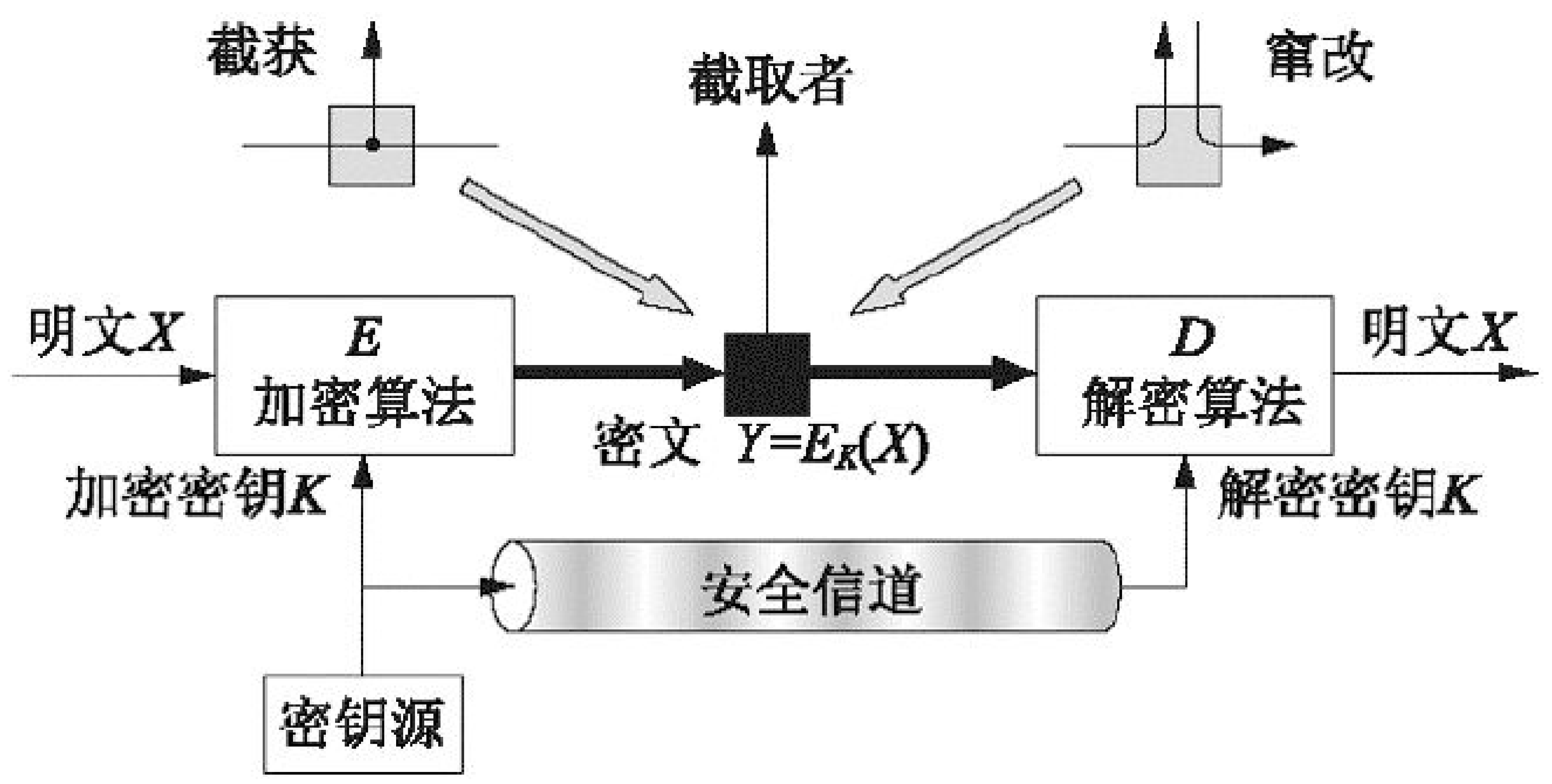


图 8-1 一般的数据加密模型

加/解密函数 E 和 D 是公开的，而密钥 K 是秘密的。在传送过程中，偷听者得到的是无法理解的密文，而他又得不到密钥，这就达到了对第三者保密的目的。

8.2.1.2 经典加密技术

经典加密方法主要使用了替换加密、换位加密和一次性填充 3 种加密技术。

(1) 替换加密：用一个字母替换另一个字母。

(2) 换位加密：按照一定的规律重排字母的顺序。

(3) 一次性填充：把明文变为位串，选择一个等长的随机位串作为密码，对二者进行按位异或，得到密文。

8.2.1.3 现代加密技术

对称密钥加密的发送和接收数据的双方必须使用相同的/对称的密钥对明文进行加密和解密运算。常用的对称加密算法有 DES、IDEA、TDEA、AES、RC2、RC4、RC5 等。

1. 数据加密标准

数据加密标准(Data Encryption Standard，DES)是 20 世纪 70 年代美国联邦注册大会上，美国国家标准局(NBS)公开征集标准密码的算法。

DES 属于分组密码体制，它将分组为 64 位的明文加密成 64 位的密文；或反之。整个加密过程由 16 个独立的加密循环构成，每一个循环使用自己的密钥 K_1，K_2，…，K_{16} 和加密函数。解密使用与加密相同的过程，但顺序与加密相反，从 K_{16} 开始变换，直至 K_1。主密钥为 56 位，用于生成每轮循环各自的密钥 K_1，K_2，…，K_{16}。加密函数是 DES 加密运算

的核心，分为扩展置换(E 盒)、S 盒置换和后变位(P 盒置换)。

DES 的加密密钥和解密密钥相同，属于对称密码体制。其安全性依赖于密钥，但目前可利用差分密码分析的思想对其选择明文攻击方法，因此 56 位的密钥长度的 DES 原则上不再是安全的。增加密钥长度和采用多重 DES 的加密是有意义的加强办法。

2. 三重 DES

三重 DES 是指使用两个密钥，执行 3 次 DES 算法，如图 8-2 所示。其密钥长度是 112 位。

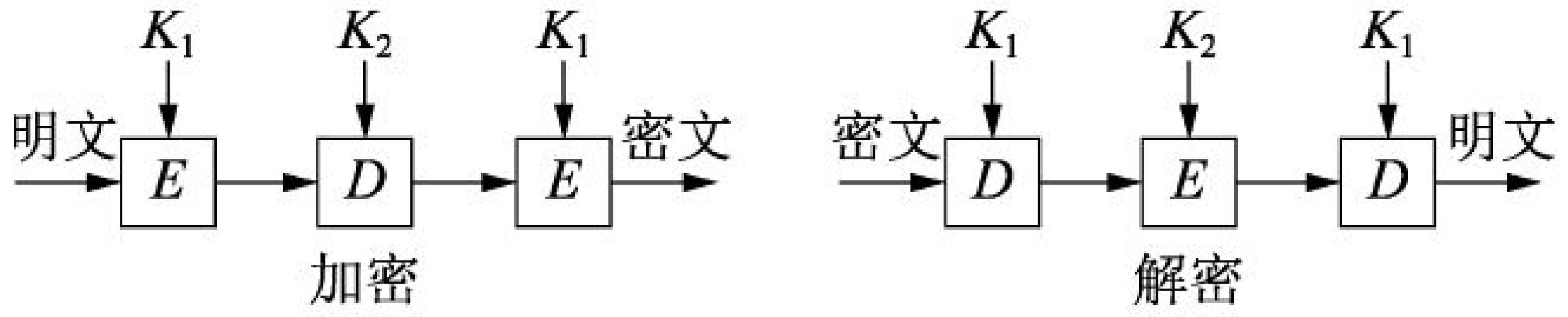


图 8-2　三重 DES 加密算法

3. 国际数据加密数据算法

国际数据加密数据算法(International Data Encryption Algorithm，IDEA)是瑞士苏黎世联邦工业大学(ETH)的 Xuejia Lai 和 James L. Massey 于 1991 年提出的。该算法形式上和 DES 类似，也是使用循环加密方式，把分组为 64 位的明文加密为 64 位的密文；或反之。所不同的是，IDEA 使用 128 位的密钥，扩展成 52 个 16 位循环密钥，安全性强于 DES。若采用强行攻击，对付 IDEA 将是对付 DES 工作量的 $2^{72}=4.7\times10^{21}$ 倍，因此，它的安全性是比较好的，是目前数据加密中应用较为广泛的一种密码体制。

由于加密密钥和解密密钥都由同一个主密钥派生而来，IDEA 仍属于对称密码体制，而且其设计倾向于软件实现，目前尚未找到破译方法。

4. 公开密钥密码体制

公开密钥密码体制也称为非对称密钥加密。每个用户都有一对密钥：公开密钥和私有密钥。公钥对外公开，私钥由个人秘密保存；用其中一把密钥来加密，另一把密钥来解密。虽然秘密密钥(SK)是由公开密钥(PK)决定的，但却不能根据 PK 计算出 SK。公开密钥密码算法原理如图 8-3 所示。

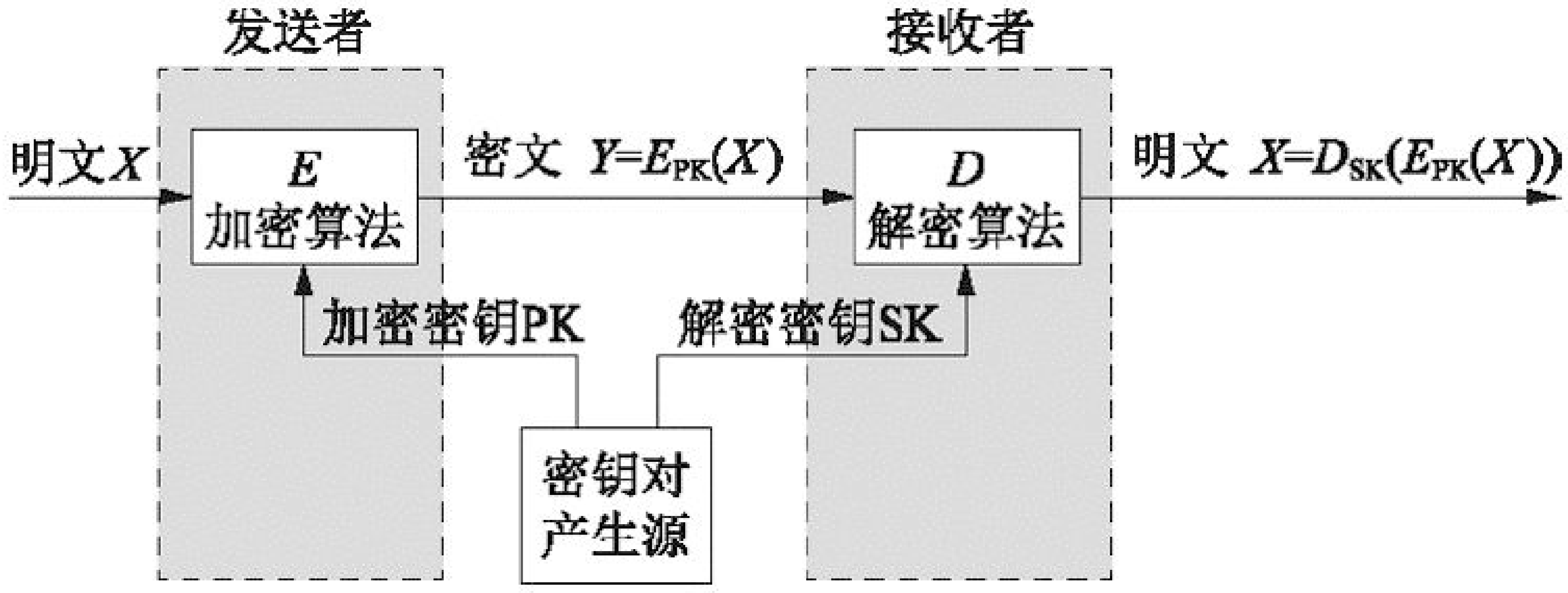


图 8-3　公开密钥密码算法

1)　RSA 算法

此算法的基础是在数论中寻求两个大素数比较简单，而将它们的乘积分解开则极其困

难。每个用户有两个密钥：加密密钥 PK = {*e*, *n*} 和解密密钥 SK = {*d*, *n*}。用户把加密密钥公开，使得系统中任何其他用户都可使用，而对解密密钥中的 *d* 则保密。*N* 为两个大素数 *p* 和 *q* 之积(素数 *p* 和 *q* 一般为 100 位以上的十进制数)，*e* 和 *d* 满足一定的关系。攻击者已知 *e* 和 *n* 时也并不能求出 *d*。

2)　其他的公钥加密算法

ElGamal 算法也是一种常用的公钥加密算法，它是基于公钥密码体制和椭圆曲线加密体系，既能用于数据加密，也能用于数字签名。

8.2.2　典型例题分析

例 8-3　PGP 是一种用于电子邮件加密的工具，可提供数据加密和数字签名服务，使用 __(37)__ 进行数据加密，使用 __(38)__ 进行数据完整性验证。(2017 年上半年真题 37、38)

(37)、(38)　A. RSA　　B. IDEA　　C. MD5　　D. SHA-1

A. RSA　　B. IDEA　　C. MD5　　D. SHA-1

解析：IDEA 叫对称加密算法，其机理是用一个 128bit 的密钥加密明文。在 PGP 中，IDEA 算法被用来加密邮件正文。而非对称加密算法(RSA)主要实现数字签名功能。

进行数据完整性验证则需要使用 MD5 算法。

答案：(37) B　(38) C

例 8-4　三重 DES 加密使用 __(41)__ 个密钥对明文进行 3 次加密，其密钥长度为 __(42)__ 位。(2017 年上半年真题 41、42)

(41) A. 1　　B. 2　　C. 3　　D. 4

(42) A. 56　　B. 112　　C. 128　　D. 168

解析：三重 DES 是指使用两个密钥，执行 3 次 DES 算法。其密钥长度是 112 位。

答案：(41) B　(42) B

例 8-5　以下加密算法中，适合对大量的报文消息进行加密传输的是 __(43)__。(2017 年上半年真题 43)

A. RSA　　B. SHA-l　　C. MD5　　D. RC5

解析：对称密钥密码体制的优点在于效率高，算法简单，系统开销小，适合加密大量数据。答案中仅有 RC5 为对称密码体制。

答案：D

例 8-6　DES 加密算法的密钥长度为 56 位，三重 DES 的密钥长度为 __(45)__ 位。(2016 年下半年真题 45)

A. 168　　B. 128　　C. 112　　D. 56

解析：三重 DES 是指使用两个密钥，执行 3 次 DES 算法，其密钥长度是 112 位。

答案：C

例 8-7　3DES 的密钥长度为 __(44)__ 位。(2016 年上半年真题 44)

A. 56　　B. 112　　C. 128　　D. 168

解析：DES 使用 56 位密钥加密。3DES 是 DES 加密算法的一种模式，它使用 3 条 56

位的密钥对数据进行 3 次加密。本质上就相当于用一个长为 168 位的密钥进行加密。若数据对安全性要求不那么高，K_1 可以等于 K_3，即第一次和第三次采用相同的密钥，在这种情况下，密钥的有效长度为 112 位。

答案：B

例 8-8　以下关于三重 DES 加密的叙述中，正确的是 (43) 。(2016 年上半年真题 43)

A. 三重 DES 加密使用一个密钥进行三次加密

B. 三重 DES 加密使用两个密钥进行三次加密

C. 三重 DES 加密使用三个密钥进行三次加密

D. 三重 DES 加密的密钥长度是 DES 密钥长度的 3 倍

解析：三重 DES 加密使用两个密钥对报文做 3 次 DES 加密，效果相当于将 DES 密钥的长度加倍，DES 密钥为 56 位，则三重 DES 的密钥长度为 112 位。

答案：B

8.2.3　同步练习

1. 高级加密标准(AES)支持的 3 种密钥长度不包括________。

   A. 56　　B. 128　　C. 192　　D. 256

2. 按照 RSA 算法，若选两奇数 p=5，q=3，公钥 e=7，则私钥 d 为________。

   A. 6　　B. 7　　C. 8　　D. 9

3. IEEE 802.11i 所采用的加密算法为______。

   A. DES　　B. 3DES　　C. IDEA　　D. AES

4. 以下关于加密算法的叙述中，正确的是________。

   A. DES 算法采用 128 位的密钥进行加密

   B. DES 算法采用两个不同的密钥进行加密

   C. 三重 DES 算法采用 3 个不同的密钥进行加密

   D. 三重 DES 算法采用 2 个不同的密钥进行加密

5. 常用对称加密算法不包括________。

   A. DES　　B. RC-5　　C. IDEA　　D. RSA

8.2.4　同步练习参考答案

1. A　　2. B　　3. D　　4. D　　5. D

8.3　认　　证

8.3.1　考点辅导

1. 基于共享密钥的认证

基于共享密钥的认证是指通信双方有一个共享的密钥，要依赖于一个双方都信赖的密钥分发中心(Key Distribution Center，KDC)。认证过程如图 8-4 所示。A 向 KDC 发出消息(这

个消息的一部分用 K_A 加密了)，说明自己要和 B 进行通信，并指出了与 B 会话的密钥 K_S。KDC 知道 A 的意图后构造一个消息发给 B，B 用 K_B 解密后就得到了 A 和 K_S，然后就可以与 A 会话了。

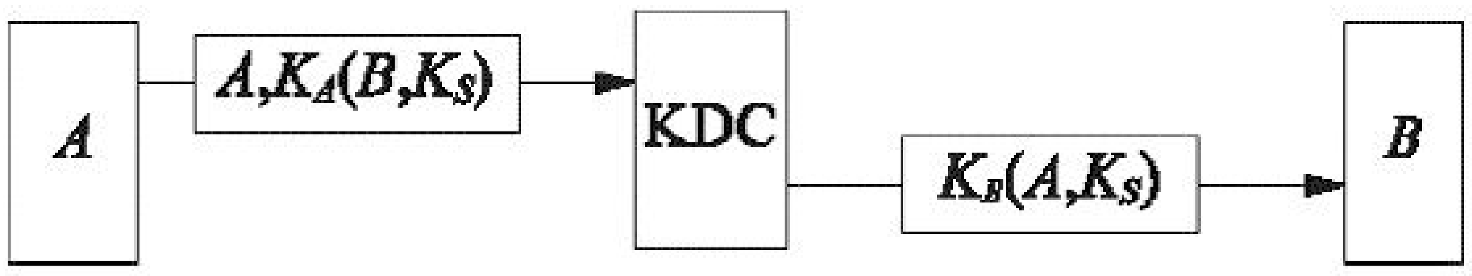


图 8-4　基于共享密钥的认证协议

2. Needham-Schroeder 认证协议

Needham-Schroeder 认证协议是一种多次提问—响应协议，可以对付重放攻击，关键是每一个会话回合都有一个新的随机数在起作用。其应答过程如图 8-5 所示。

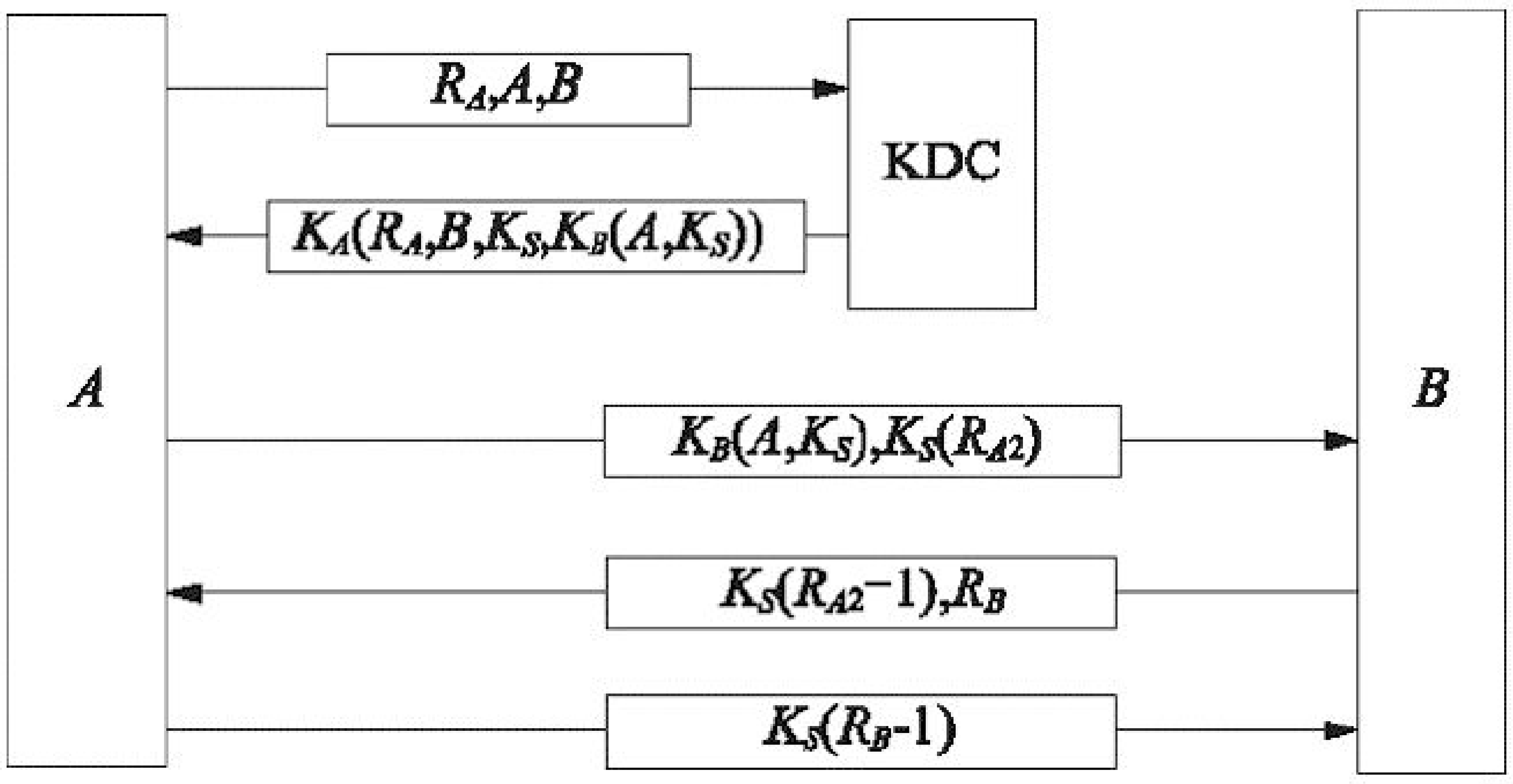


图 8-5　Needham-Schroeder 认证协议

3. 基于公钥的认证

基于公钥的认证是指通信双方都用对方的公钥加密，用各自的私钥解密。具体过程如图 8-6 所示。通信报文中有 A 和 B 指定的随机数 R_A 和 R_B，因此能排除重放的可能性。

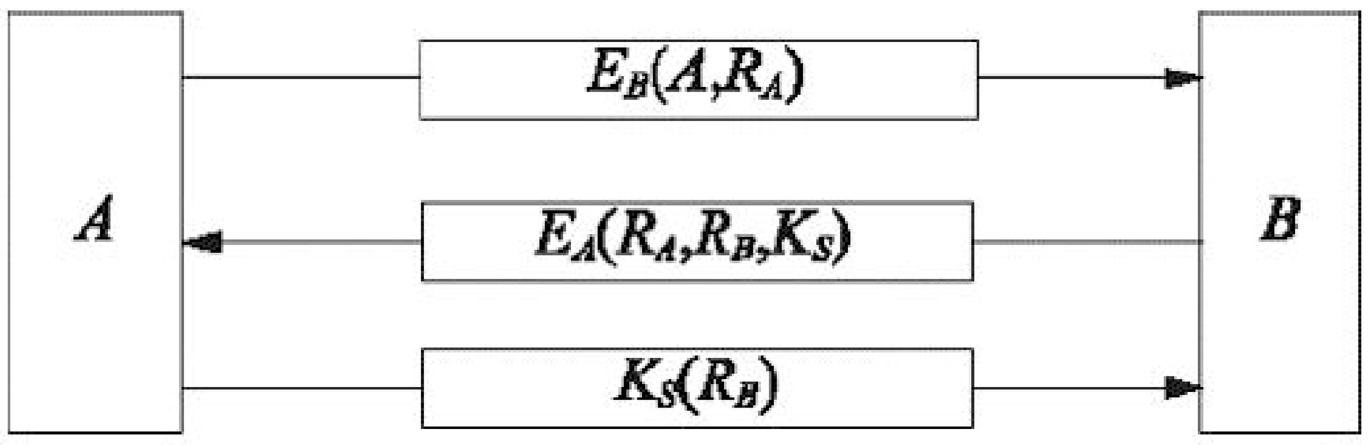


图 8-6　基于公钥的认证协议

8.3.2　典型例题分析

例 8-9　假定用户 A、B 分别在 I1 和 I2 两个 CA 处取得了各自的证书，下面________是 A、B 互信的必要条件。

A. A、B 互换私钥　　　　B. A、B 互换公钥

C. I1、I2 互换私钥　　　D. I1、I2 互换公钥

解析：两个用户分别取得证书之后，两个 CA 相互交换 CA 的公钥来验证对方身份。

答案：D

例 8-10　IIS 8.0 支持的身份验证安全机制有 4 种验证方法，其中安全级别最高的验证方法是______。

A. 匿名身份验证　　B. 集成 Windows 身份验证

C. 基本身份验证　　D. 摘要式身份验证

解析：如果启用了匿名访问，访问站点时，不要求提供经过身份验证的用户凭据；集成 Windows 身份验证以 Kerberos 票证的形式通过网络向用户发送身份验证信息，并提供较高的安全级别；基本身份验证需要用户 ID 和密码，提供的安全级别较低；Windows 域服务器的摘要式身份验证需要用户 ID 和密码，可提供中等的安全级别。

答案：B

8.3.3　同步练习

基于共享密钥的认证，通信双方有一个共享的密钥，要依赖于一个双方都信赖的________。

A. KDC　　B. KDA　　C. SDC　　D. KAC

8.3.4　同步练习参考答案

A

8.4　数 字 签 名

8.4.1　考点辅导

1. 基于密钥的数字签名

基于密钥的数字签名系统中要有收、发双方共同信赖的仲裁人，如图 8-7 所示。其中，BB 是 A 和 B 共同信赖的仲裁人，K_A 和 K_B 分别是 A 和 B 与 BB 之间的密钥，K_{BB} 是只有 BB 掌握的密钥，P 是 A 发给 B 的消息，t 是时间戳。由 BB 解读 A 发的报文，然后产生一个签名的消息 $K_{BB}(A,t,P)$，并装配成发给 B 的报文；B 可以解密该报文，阅读消息 P，并保留证据。

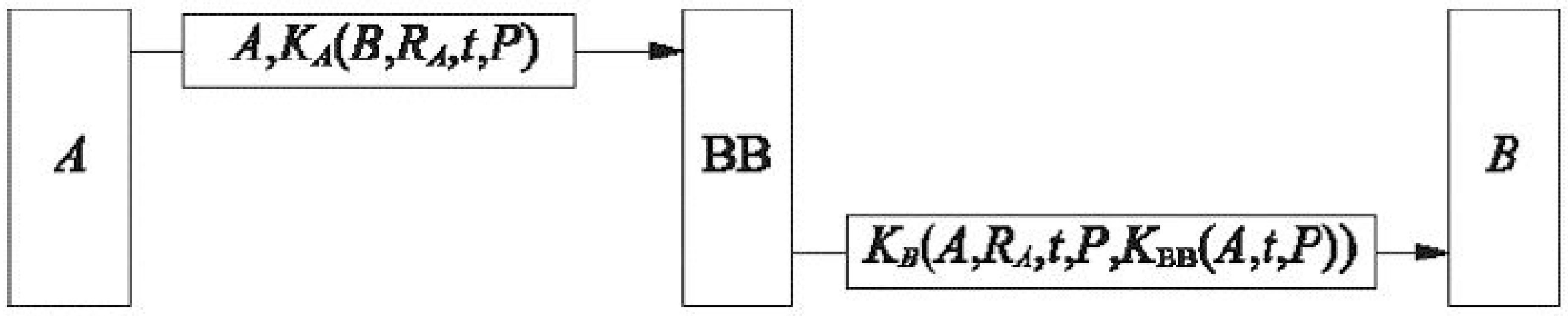


图 8-7　基于密钥的数字签名

2. 基于公钥的数字签名

利用公钥加密算法的数字签名系统如图 8-8 所示。这样的签名方法是符合可靠性原则的，即：签字是可以被确认的；签字是无法被伪造的；签字是无法重复使用的；文件被签字以后是无法被窜改的；签字具有无可否认性。如果 A 方否认了，B 可以拿出 $D_A(P)$，并用 A 的公钥 E_A 解密得到 P，从而证明 P 是 A 发送的；如果 B 把消息窜改了，当 A 要求 B 出示原来的 $D_A(P)$时，B 拿不出来。

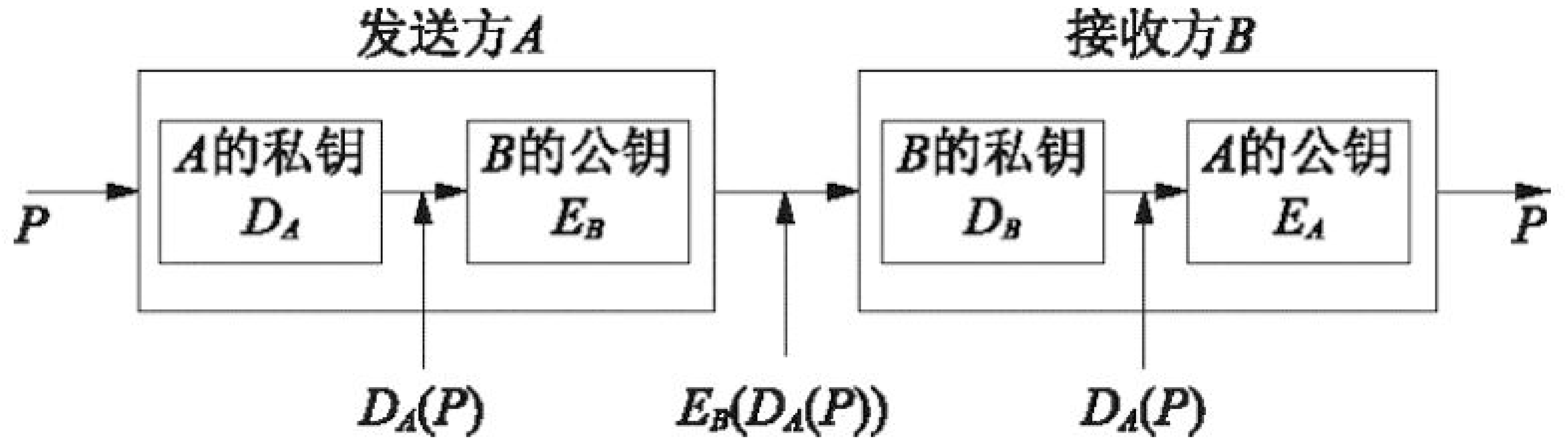


图 8-8　基于公钥的数字签名

8.4.2　典型例题分析

例 8-11　下面不属于数字签名的作用的是__(43)__。(2016 年下半年真题 43)

A. 接收者可验证消息来源的真实性

B. 发送者无法否认发送过该消息

C. 接收者无法伪造、窜改信息

D. 可验证接收者的合法性

解析：数字签名应该满足以下条件：①接收者能够核实发送者；②发送者事后不能抵赖对报文的签名；③接收者不能伪造对报文的签名。

答案：D

例 8-12　用户 B 收到经 A 数字签名后的消息 M，为验证消息的真实性，首先需要从 CA 获取用户 A 的数字证书，该数字证书中包含__(41)__，可以利用__(42)__验证该证书的真伪，然后利用__(43)__验证 M 的真实性。(2016 年上半年真题 41～43)

(41) A. A 的公钥　　B. A 的私钥　　C. B 的公钥　　D. B 的私钥

(42)、(43)A. CA 的公钥　　B. B的私钥　　C. A 的公钥　　D. B的公钥

解析：数字证书颁发的过程为：用户首先产生自己的密钥对，并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实从用户而来，然后认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和他的公钥，同时还附有认证中心的签名信息，用户可以利用认证中心 CA 的公钥验证该证书的真伪。而数字签名是发送方用自己的私钥对信息进行签名，接收方用发送方的公钥对信息进行核实签名。

答案：(41) A　(42) A　(43) C

例 8-13　下列算法中，可用于报文认证的是__(42)__，可以提供数字签名的是__(43)__。(2015 年下半年真题 42、43)

(42)、(42)　A. RSA　　B. IDEA　　C. RC4　　D. MD5

解析：报文认证是为了确保数据的完整性和真实性，对报文的来源、时间及目的地进行验证。报文的认证方式有传统加密方式的认证、使用密钥的报文认证码方式、使用单向散列函数的认证和数字签名认证方式。常用于报文认证的算法有 MD5 和 SHA。MD5(Message Digest algorithm 5)是一种单向散列算法，可以把不同长度的数据块进行暗码运算产生一个 128 位的数值；SHA(Secure Hash Algorithm)是一种较新的散列算法，可以对任意长度的数据进行运算生成一个 160 位的数值。

数字签名是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir、Des/DSA 及椭圆曲线数字签名算法和有限自动机数字签名算法等。

答案：(42) D　(43) A

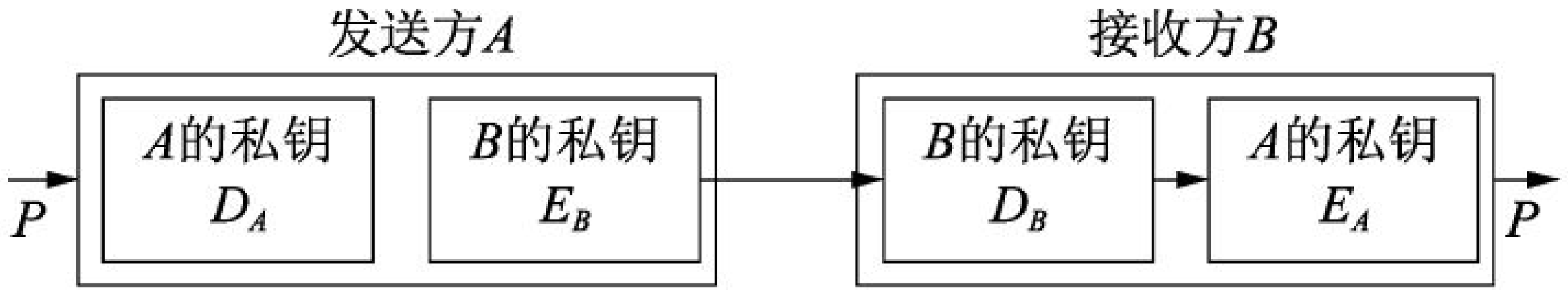
8.4.3　同步练习

1.　公钥体系中，私钥用于__(1)__，公钥用于__(2)__。

(1)、(2)　A. 解密和签名　　B. 加密和签名

C. 解密和认证　　D. 加密和认证

2.　下图所示为一种数字签名方案，网上传送的报文是__(1)__，防止 A 抵赖的证据是__(2)__。



(1)、(2)　A. P　　B. $D_A(P)$　　C. $E_B(D_A(P))$　　D. D_A

3.　报文摘要算法 MD5 的输出是__(1)__位，SHA-1 的输出是__(2)__位。

(1)、(2)　A. 56　　B. 128　　C. 160　　D. 168

4.　某报文的长度是 1000 字节，利用 MD5 计算出来的报文摘要长度是__(1)__位，利用 SHA 计算出来的报文摘要长度是__(2)__位。

(1)、(2)　A. 64　　B. 128　　C. 256　　D. 160

5.　Alice 向 Bob 发送数字签名的消息 M，则不正确的说法是______。

A. Alice 可以保证 Bob 收到消息 M

B. Alice 不能否认发送过消息 M

C. Bob 不能编造或改变消息 M

D. Bob 可以验证消息 M 确实来源于 Alice

6.　安全散列算法 SHA-1 产生的摘要的位数是_____。

A. 64　　B. 128　　C. 160　　D. 256

7.　数字签名功能不包括______。

A. 防止发送方的抵赖行为　　B. 发送方身份确认

C. 接收方身份确认　　　　　　　　D. 保证数据的完整性

8.4.4　同步练习参考答案

1. (1) A　(2) D　2. (1) C　(2) B　3. (1) B　(2) C
4. (1) B　(2) D　5. A　6. C　7.C

8.5　报 文 摘 要

8.5.1　考点辅导

1. 报文摘要算法

MD5 是 MIT 的 Ron Rivest(RFC 1321)提出的。算法以任意长的报文作为输入，算法的输出是产生一个 128 位的报文摘要。输出的摘录用 4 个字 d_0、d_1、d_2、d_3 表示，在计算开始时分别初始化为常数，然后一直参与算法，其值不断被改编，直到作为最后结果输出。

最初值：d_0=01234567H，d_1=89abcdefH，d_2=fedcba98H，d_3=76543210H。

输入报文首先被填充，使其成为 16 的倍数，然后被分成 512bit 的等长块，逐块处理。每块处理分 4 遍扫描，在每遍扫描时对 d_0、d_1、d_2、d_3 使用不同的扰乱函数。扰乱函数将报文的分组和相应 d_i 进行函数运算，这样每遍扫描将每个 d_0、d_1、d_2、d_3 报文内容进行了更新。在处理前将当前摘录备份，在处理后将这个备份加到新产生的信息摘录上，并将其作为下一块处理时的摘录当前值。最后一块信息处理之后的信息摘录 d_0、d_1、d_2、d_3 当前值，即为最终的信息摘录值。

扰乱函数计算使用了取整、二进制求补、二进制与运算、二进制或运算、半加运算、二进制加运算和循环左移运算等。

2. 安全散列算法

安全散列算法(Secure Hash Algorithm，SHA)由美国国家标准和技术协会于 1993 年提出，并被定义为安全散列标准(Secure Hash Standard，SHS)。SHA-1 是 1994 年修订的版本，纠正了 SHA 一个未公布的缺陷。这种算法接收的输入报文小于 2^{64} 位，产生 160 位的报文摘要。该算法设计的目标是使得找出一个能够匹配给定的散列值的文本实际是不可能计算的。也就是说，如果对文档 A 已经计算出了散列值 H(A)，那么很难找到一个文档 B，使其散列值 H(B)=H(A)，尤其困难的是无法找到满足上述条件的而且又是指定内容的文档 B。SHA 算法的缺点是速度比 MD5 慢，但是 SHA 的报文摘更长，更有利于对抗野蛮攻击。

3. 散列式报文认证码

散列式报文认证码(HMAC)是利用对称密钥产生报文认证码的散列算法，可以提供数据完整性、数据源身份认证。

HMAC 使用现有的散列函数 H 而不用修改其代码，这样可以使用已有的 H 代码库，而

且可以随时用一个散列函数代替另一个散列函数。HMAC-MD5 已经被 IETF 指定为 Internet 安全协议 IPSec 的验证机制，提供数据源认证和数据完整性保护。

8.5.2 典型例题分析

例 8-14 SHA-l 是一种将不同长度的输入信息转换成__(45)__位固定长度摘要的算法。(2017 年上半年真题 45)

A. 128　　B. 160　　C. 256　　D. 512

解析： RFC 1321 提出的报文摘要算法 MD5 已经获得广泛的应用。它可对任意长度的报文进行运算，得出 128 位的 MD5 报文摘要代码。另一种标准是安全散列算法 SHA，和 MD5 相似，但码长为 160 位，SHA 比 MD5 更安全，但计算的效率不如 MD5。

答案： B

例 8-15 下面可用于消息认证的算法是__(44)__。(2016 年下半年真题 44)

A. DES　　B. PGP　　C. MD5　　D. KMI

解析： 报文摘要算法 MD5 已获得了广泛的应用，它可对任意长度的报文进行运算，得出 128 位的 MD5 报文摘要代码。除此之外还有一种和 MD5 相似的安全散列算法 SHA，码长为 160 位，比 MD5 更安全，但计算效率不及 MD5。

答案： C

例 8-16 下列不属于报文认证算法的是__(45)__。(2016 年上半年真题 45)

A. MD5　　B. SHA-1　　C. RC4　　D. HMAC

解析： RC4 加密算法是 1987 年设计的密钥长度可变的流加密算法簇，是一种对称加密算法。该算法的速度可以达到 DES 加密算法的 10 倍左右，且具有很高级别的非线性。是应用最广泛的流加密算法，应用在安全套接字层(SSL)(用来保护网络上传输的数据)和 WEP(无线网络数据保护)上。

RFD 1321 提出的报文摘要算法 MD5 已获得广泛的应用，它可对任意长度的报文进行运算，得出 128 位的 MD5 报文摘要代码。还有一种安全散列算法(SHA)，和 MD5 相似但码长为 160 位。SHA 比 MD5 更安全，但效率较低。另外还有 HAMC(散列消息鉴别码)，是基于密钥的 Hash 算法的认证协议。其原理为：用公开函数和密钥产生一个固定长度的值作为认证标识，用此标识来验证消息的完整性，使用一个密钥生成一个固定大小的小数据块，即 MAC，并将其加入到消息中，然后传输。接收方利用与发送方共享的密钥进行鉴别认证。

答案： C

8.5.3 同步练习

1. 在报文摘要算法 MD5 中，首先要进行明文分组与填充，其中分组时明文报文要按照________位分组。

　A. 128　　B. 256　　C. 512　　D. 1024

2. 报文摘要算法 MD5 的输出是__(1)__位，SHA-1 的输出是__(2)__位。

(1)、(2)　A. 56　　B. 128　　C. 160　　D. 168

3. 某报文的长度是 1000 字节，利用 MD5 计算出来的报文摘要长度是__(1)__位，利用 SHA 计算出来的报文摘要长度是__(2)__位。

(1)、(2) A. 64　　B. 128　　C. 256　　D. 160

8.5.4 同步练习参考答案

1. C　2. (1) B　(2) C　3. (1) B　(2) D

8.6 数 字 证 书

8.6.1 考点辅导

1. 数字证书的概念

数字证书解决了公开密钥密码体制下密钥的发布和管理问题。用户可以公开其公钥，而保留其私钥。一般包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。

数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心(CA)作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。目前得以广泛使用的证书标准是 X.509。表 8-1 所示为 X.509 数字证书中的各个数字域的含义。

表 8-1　X.509 数字证书中的各个数字域的含义

域	含　义
版本号	证书版本号，不同版本的证书格式不同
序列号	序列号，同一身份验证机构签发的证书序列号唯一
签名算法	签署证书所用的签名算法，包括必要的参数
发行者	建立和签署证书的 CA 名称
有效期	包括有效期的起始时间和终止时间
主体名	证书持有人的名称，以及这一证书用来证明私钥用户对应的公开密钥
主体的公钥	主体的公开密钥、使用这一公开密钥的算法的标识符及参数
发行者唯一标识符	(可选)证书颁发者的唯一标识符
主体唯一标识符	(可选)证书拥有者的唯一标识符
扩充域	(可选)可选的标准和专用功能字段，如基本限制字段和密钥用法字段
签名	CA 用自己的私钥对上述域的哈希值进行数字签名的结果

2. 证书的获取

任何一个用户要得到 CA 的公钥，就能得到该 CA 为该用户签署的公钥。由于证书是不可伪造的，因此对于存放证书的目录无须施加特别的保护。

由于一个公钥用户拥有的可信任管理中心数量有限，要与大量不同管理域的用户建立安全通信需要 CA 间建立信任关系。一个证书链是从一个自签名的根证书开始，前一个证书主体是后一个证书的发放者。也就是说，该主体对后一个证书进行签名。一般来说，对证

书链的处理需要考虑每个证书相关的信任关系。

3. 证书的吊销

用户的数字到了有效期的终止时间、用户私钥已被泄露、用户放弃使用原 CA 的服务、CA 私钥泄露都需要吊销用户的数字证书。为此，CA 维护有一个证书吊销列表(CRL)，以供用户查询。

8.6.2 典型例题分析

例 8-17　下列说法错误的是________。

A. 不同版本的证书格式不同

B. 同一身份验证机构签发的证书序列号不唯一

C. 有效期包括有效期的起始时间和终止时间

D. 发行者是建立和签署证书的 CA 名称

解析：同一身份验证机构签发的证书序列号唯一。

答案：B

8.6.3 同步练习

1.　假设有证书发放机构 I1、I2，用户 A 在 I1 获取证书，用户 B 在 I2 获取证书，I1 和 I2 已安全交换了各自的公钥，如果用 I1《A》表示由 I1 颁发给 A 的证书，A 可通过________证书获取 B 的公开密钥。

A. I1《I2》I2《B》　　B. I2《B》I1《I2》

C. I1《B》I2《I2》　　D. I2《I2》I2《B》

2.　目前得以广泛使用的证书标准是________。

A. X.509　　B. X.508　　C. X.506　　D. X.507

3.　某网站向 CA 申请了数字证书。用户通过 (1) 来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过 (2) 进行加密和验证，该网站通过 (2) 进行解密和签名。

(1)、(2)、(3) A. CA 的签名　　B. 证书中的公钥

C. 网站的私钥　　D. 用户的公钥

4.　在 X.509 标准中，不包含在数字证书中的数据域是____。

A. 序列号　　B. 签名算法

C. 认证机构的签名　　D. 私钥

8.6.4 同步练习参考答案

1. A　　2. A　　3. (1) A　(2) B　(3) C　　4. D

8.7　密 钥 管 理

8.7.1　考点辅导

8.7.1.1　密钥管理概述

1. 对密钥的威胁

对密钥的威胁有以下几种。

(1)　私钥的泄露。

(2)　私钥或公钥的真实性(Authenticity)丧失。

(3)　私钥或公钥未经授权使用，如使用失效的密钥或违例使用密钥。

2. 密钥的种类

有如下几种密钥。

(1)　基本密钥 K_p：这是由用户选定或由系统分配给用户的、可在较长时间(相对于会话密钥)内由一对用户所专用的密钥，故也称为用户密钥。基本密钥要求既安全又便于更换，与会话密钥一起去启动和控制某种算法所构造的密钥产生器，生成用于加密数据的密钥流。

(2)　会话密钥 K_s：这是两个终端用户在交换数据时使用的密钥。当用会话密钥对传输的数据进行保护时称为数据加密密钥，用会话密钥来保护文件时称为文件密钥。会话密钥的作用是使用户不必频繁地更换基本密钥，有利于密钥的安全和管理。会话密钥可由用户双方预先约定，也可由系统通过密钥建立协议动态地生成并分发给通信双方。K_s 使用时间短，限制了密码分析者所能得到的同一密钥加密的密文数量。会话密钥只在需要时通过协议建立，也降低了密钥的存储容量。

(3)　密钥加密密钥 K_e：这是用于对传送的会话密钥或文件密钥进行加密的密钥，也称辅助二级密钥或密钥传送密钥。通信网中每个节点都分配有一个 K_e，为了安全，各节点的 K_e 应互不相同。

(4)　主机密钥 K_m：这是对密钥加密密钥进行加密的密钥，存于主机处理器中。

(5)　在双钥体制下，有公开钥(公钥)和秘密钥(私钥)、签字密钥和认证密钥之分。

8.7.1.2　密钥管理体制

密钥管理是信息安全的核心技术之一。在美国信息保障技术框架(Information Assurance Technical Framework，IATF)中定义的密钥管理体制主要有 3 种：一是适用于封闭网，以传统的密钥分发中心为代表的 KMI 技术；二是适用于开放网的 PKI 技术；三是适用于规模化专用网的 SPK 技术。

1. KMI 技术

密钥管理基础结构(Key Management Infrastructure，KMI)假定有一个密钥分发中心(KDC)来负责发放密钥。这种结构经历了从静态分发到动态分发的发展历程，目前仍然是密钥管理的主要手段。无论是静态分发还是动态分发，都是基于秘密的物理通道进行的。

1) 静态分发

静态分发是预配置技术，大致有以下几种。

(1) 点对点配置。可用单钥实现，也可用双钥实现。单钥分发是最简单而有效的密钥管理技术，通过秘密的物理通道实现。单钥为认证提供可靠的参数，但不能提供不可否认性服务。有数字签名要求时则用双钥实现。

(2) 一对多配置。可用单钥或双钥实现，是点对点分发的扩展，只是在中心保留所有各端的密钥，而各端只保留自己的密钥。一对多的密钥分配在银行清算、军事指挥、数据库系统中仍为主流技术，也是建立秘密通道的主要方法。

(3) 格状网配置。可以用单钥实现，也可以用双钥实现。格状网的密钥配置量为全网 n 个终端用户中选 2 的组合数。Kerberos 曾安排过 25 万个用户的密钥。格状网一般都要求提供数字签名服务，因此多数用双钥实现，即各端保留自己的私钥和所有终端的公钥。如果用户量为 25 万个，则每一个终端用户要保留 25 万个公钥。

2) 动态分发

动态分发是“请求—分发”机制，是与物理分发相对应的电子分发，在秘密通道的基础上进行，一般用于建立实时通信中的会话密钥，在一定意义上缓解了密钥管理规模化的矛盾。动态分发有以下两种形式。

(1) 基于单钥的单钥分发。在用单密钥实现时，首先在静态分发方式下建立星状密钥配置，在此基础上解决会话密钥的分发。这种密钥分发方式简单易行。

(2) 基于单钥的双钥分发。在双钥体制下，可以将公、私钥都当作秘密变量，也可以将公、私钥分开，只把私钥当作秘密变量，公钥当作公开变量。尽管将公钥当作公开变量，但仍然存在被假冒或窜改的可能，因此需要有一种公钥传递协议，证明其真实性。基于单钥的公钥分发的前提是密钥分发中心(C)和各终端用户(A、B)之间已存在单钥的星状配置，分发过程如下。

G A_C：申请 B 的公钥，包括 A 的时间戳。

G C_A：将 B 的公钥用单密钥加密发送，包括 A 的时间戳。

G A_B：用 B 的公钥加密 A 的身份标识和会话序号 N1。

G B_C：申请 A 的公钥，包括 B 的时间戳。

G C_B：将 A 的公钥用单密钥加密发送，包括 B 的时间戳。

G B_A：用 A 的公钥加密 A 的会话序号 N1 和 B 的会话序号 N2。

G A_B：用 B 的公钥加密 N2，以确认会话建立。

2. PKI 技术

在密钥管理中，不依赖秘密信道的密钥分发技术一直是一个难题。1976 年，Deffie 和 Hellman 提出了双钥密码体制和 D-H 密钥交换协议，大大促进了这一领域的进程。但是，在双钥体制中只是有了公、私钥的概念，私钥的分发仍然依赖于秘密通道。1991 年，PGP 首先提出了 Web of Trust 信任模型和密钥由个人产生的思路，避开了私钥的传递，从而避开了秘密通道，推动了 PKI 技术的发展。

公钥基础结构(Public Key Infrastructure，PKI)是运用公钥的概念和技术来提供安全服务的、普遍适用的网络安全基础设施，包括由 PKI 策略，软、硬件系统，认证中心(CA)，注

册机构(RA)，证书签发系统和 PKI 应用等构成的安全体系，如图 8-9 所示。

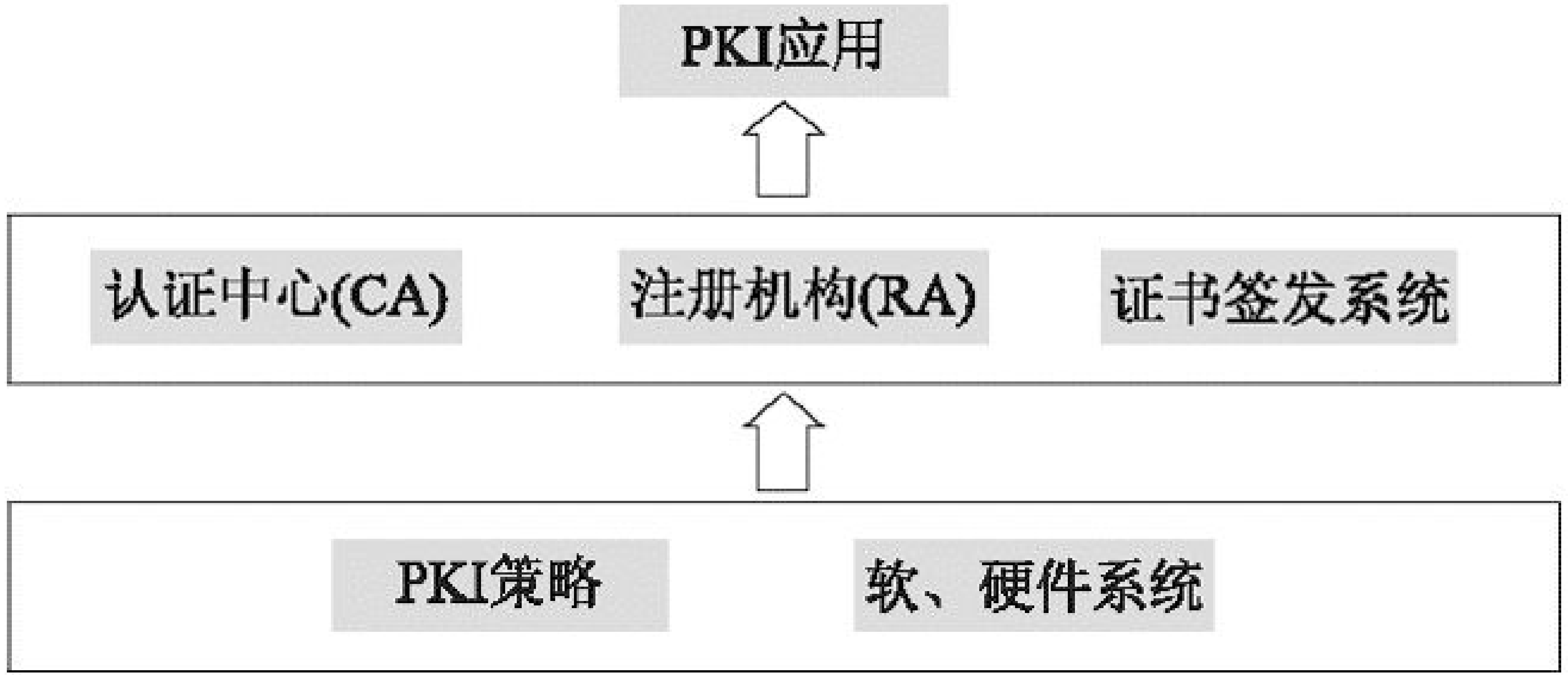


图 8-9　PKI 的组成

PKI 策略定义了信息安全的指导方针和密码系统的使用规则，具体内容包括 CA 之间的信任关系、遵循的技术标准、安全策略、服务对象、管理框架、认证规则、运作制度、所涉及的法律关系等；软、硬件系统是 PKI 运行的平台，包括认证服务器、目录服务器等；认证中心(Certificate Authority，CA)负责密钥的生成和分配；注册机构(Registration Authority，RA)是用户(Subscriber)与 CA 之间的接口，负责对用户的认证；证书签发系统负责公钥数字证书的分发，可以由用户自己或通过目录服务器进行发放； PKI 的应用非常广泛，包括 Web 通信、电子邮件、电子数据交换、电子商务、网上信用卡交易、虚拟专用网等都是 PKI 潜在的应用领域。

20 世纪 90 年代以来，PKI 技术逐渐得到了各国政府和许多企业的重视，由理论研究进入商业应用阶段。IETF 和 ISO 等国际组织陆续颁布了 X.509、PKIX、PKCS、S/MIME、SSL、SET、IPSec、LDAP 等一系列与 PKI 应用有关的标准；RSA、VeriSign、Entrust、Baltimore 等网络安全公司纷纷推出了 PKI 产品和服务；网络设备制造商和软件公司开始在网络产品中增加 PKI 功能；美国、加拿大、韩国、日本和欧盟等国家相继建立了 PKI 体系；银行、证券、保险和电信等行业的用户开始接受和使用 PKI 技术。

PKI 解决了不依赖秘密信道进行密钥管理的重大课题，但这只是概念的转变，并没有多少新技术。PKI 是在民间密码研究摆脱政府控制的斗争中发展起来的，而这种斗争一度达到了白热化程度，PGP 的发明者 Philip Zimmermann 曾经因为违反美国的密码产品贸易管制政策而被联邦政府调查。PKI 以商业运作的形式壮大起来，以国际标准的形式确定。PKI 技术完全开放，甚至连一向持反对态度的美国国防部(DoD)、联邦政府也不得不开发 PKI 策略。DoD 定义的 KMI/PKI 标准规定了用于管理公钥证书和对称密钥的技术、服务和过程，KMI 是提供信息保障能力的基础架构，而 PKI 是 KMI 的主要组成部分，提供了生成、生产、分发、控制和跟踪公钥证书的服务框架。

KMI 和 PKI 两种密钥管理体制各有其优、缺点和适用范围：①KMI 具有很好的封闭性，而 PKI 则具有很好的扩展性。②KMI 的密钥管理机制可形成各种封闭环境，可作为网络隔离的基本逻辑手段；而 PKI 则适用于各种开放业务，但却不适应封闭的专用业务和保密性业务。③KMI 是集中式的基于主管方的管理模式，为身份认证提供直接信任和一级推理信任，但密钥更换不灵活；PKI 是依靠第三方的管理模式，只能提供一级以下推理信任，但密钥更换非常灵活。④KMI 适用于保密网和专用网；而 PKI 则适用于安全责任完全由个人或单方面承担，安全风险不涉及他方利益的场合。

从实际应用方面看，互联网中的专用网主要处理内部事务，同时要求与外界联系。因此，KMI 主内、PKI 主外的密钥管理结构是比较合理的。如果一个专用网是与外部没有联系的封闭网，那么仅有 KMI 就已足够。如果一个专用网可以与外部联系，那么要同时具备两种密钥管理体制，至少 KMI 要支持 PKI。如果是开放网业务，则完全可以用 PKI 技术处理。

8.7.2 典型例题分析

例 8-18 Kerberos 是一种__(42)__。(2015 年上半年真题 42)

A. 加密算法　　B. 签名算法　　C. 认证服务　　D. 病毒

解析： Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无须基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下，Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术(如共享密钥)执行认证服务的。

答案： C

例 8-19 下列密钥英文简称对应错误的是________。

A. 基本密钥 K_p　　B. 会话密钥 K_s

C. 密钥加密密钥 K_e　　D. 主机密钥 K_e

解析： 主机密钥对应的英文简称为 K_m。

答案： D

8.7.3 同步练习

1. 下列不是静态分发的是________。

A. 点对点配置　　B. 一对多配置

C. 格状网配置　　D. 基于单钥的单钥分发

2. 在 Kerberos 系统中，使用一次性密钥和______来防止重放攻击。

A. 时间戳　　B. 数字签名　　C. 序列号　　D. 数字证书

3. 两个公司希望通过 Internet 传输大量敏感数据，从信息源到目的地之间的传输数据以密文形式出现，而且不希望由于在传输节点使用特殊的安全单元而增加开支，最合适的加密方式是__(1)__，使用会话密钥算法效率最高的是__(2)__。

(1) A. 链路加密　　B. 节点加密　　C. 端—端加密　　D. 混合加密

(2) A. RSA　　B. RC-5　　C. MD5　　D. ECC

8.7.4 同步练习参考答案

1. D　2. A　3. (1) C　(2) B

8.8　虚拟专用网

8.8.1　考点辅导

8.8.1.1　虚拟专用网的工作原理

虚拟专用网 (Virtual Private Network，VPN)是一种利用公共网络来构建的专用网络技术。用于构建 VPN 的公共网络包括 Internet、帧中继、ATM 等。“虚拟”这一概念是相对传统专用网络的构建方式而言的，对于广域网连接，传统的组网方式通过远程拨号连接来实现，而 VPN 是利用服务提供商所提供的公共网络来实现远程的广域连接。

通常 VPN 整合了范围广泛的客户，从家庭的拨号上网用户到办公室的联网的工作站，直到 ISP 的 Web 服务器。客户类型、传输方法以及服务的混合使用增加了 VPN 的设计复杂性，同时也增加了安全需要的复杂性，安全考虑必须同时顾及 VPN 使用的硬件设计和软件。

1. 实现 VPN 的关键技术

实现 VPN 的关键技术主要有隧道技术、加/解密技术、密钥管理技术和身份认证技术。

(1) 隧道技术是一种通过使用因特网基础设施在网络之间传递数据的方式。隧道协议将其他协议的数据封装在新的报头中发送。新的报头提供了路由信息，从而使封装的负载数据能够通过因特网传递。

(2) VPN 可以利用已有的加密技术实现保密通信，保证公司业务和个人通信的安全。

(3) 密钥管理负责密钥的生成、分发、控制和跟踪以及验证密钥的真实性等。

(4) 通常使用用户名和密码，或者智能卡实现用户的身份认证。

2. VPN 的解决方案

VPN 的解决方案有以下 3 种。

(1) Access VPN。用于远程用户需要及时地访问 Intranet 和 Extranet，如出差流动员工、远程办公人员和远程小办公室，通过公用网络与企业的 Intranet 和 Extranet 建立私有的网络连接。通常利用二层网络隧道技术建立 VPN 隧道连接来传输私有网络数据。

(2) Intranet VPN。通过公用网络进行企业各个分布点互联，是传统的专线网或其他企业网的扩展或替代形式。

(3) Extranet VPN。通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络相同的政策，包括安全、服务质量(QoS)、可管理性和可靠性。

8.8.1.2　第二层隧道协议

虚拟专用网可以通过第二层隧道协议实现，这些隧道协议都是把数据封装在点对点协议(PPP)的帧中在因特网上传输的。下面介绍点对点协议和常用的第二层隧道协议。

1. 点对点协议

点对点协议(Point to Point Protocol，PPP)是 IETF 推出的点到点类型线路的数据链路层协议。它解决了 SLIP 中的问题，并成为正式的因特网标准。

PPP 定义 PAP 和 CHAP 两种认证方式，同级系统可以使用这两种认证方式相互进行标识。

2. 点对点隧道协议

点对点隧道协议(PPTP)是一种第二层隧道协议。为了传输来自不同网络的数据包，最普遍使用的方法是先把各种网络协议(IP、IPX 和 AppleTalk 等)封装到 PPP 中，再把这整个数据包装入隧道协议中。这种双层封装形成的数据包需靠第二层协议进行传输，所以称之为“第二层隧道”。

PPTP 定义了由 PAC 和 PNS 组成的客户端/服务器结构，从而把 NAS 的功能分解给这两个逻辑设备，以支持虚拟专用网。

- PAC(PPTP Access Concentrator，PPTP 接入集中器)可以连接一条或多条 PSTN 或 ISDN 拨号线路，能进行 PPP 操作，并能处理 PPTP 协议。
- PNS(PPTP Network Server，PPTP 网络服务器)是建立在通用服务器平台上的 PPTP 服务器，运行 TCP/IP 协议，可以使用任何 LAN 和 WAN 接口硬件实现。

基于 PPTP 协议(点对点隧道协议)网络连接方式的 VPN，允许一台客户机通过一个公共网络(如 Internet)建立一个秘密的多协议 VLAN 网络。因此，它可以使得公司远端的员工通过 Internet 而不是直接拨号连接公司的网络。这就是说，通过 PPTP 的封装，可以使非 IP 网络获得 Internet 通信的优点。PPTP 是微软和其他厂家支持的标准，它是 PPP 协议的扩展，可以通过 Internet 建立多协议 VPN。

3. 第二层隧道协议

第二层隧道协议(Layer 2 Tunneling Protocol，L2TP)是一种基于点对点协议(PPP)的二层隧道协议。L2TP 扩展了 PPP 模型，允许第二层连接端点和 PPP 会话端点驻在由分组交换网连接的不同设备中。L2TP 的典型结构如图 8-10 所示。其中，LAC 表示 L2TP 访问集中器，是附属在交换网络上的具有接入功能和 L2TP 协议处理能力的设备；LNS 是 L2TP 网络服务器，是用于处理 L2TP 协议服务器端部分的软件。在一个 LNS 和 LAC 对之间存在两种类型的连接，一种是隧道(Tunnel)连接，它定义了一个 LNS 和 LAC 对；另一种是会话(Session)连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。

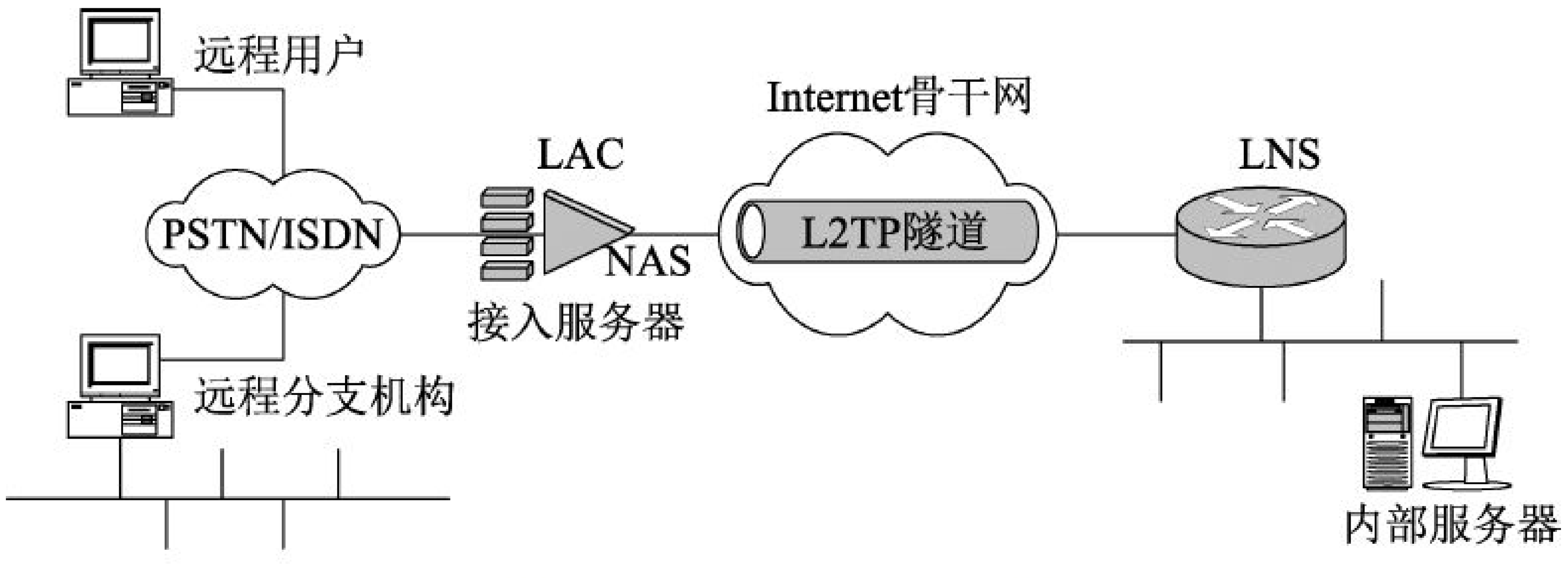


图 8-10　L2TP 的典型结构

8.8.1.3　IPSec 安全协议

IPSec 安全协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括认证报头(Authentication Header，AH)协议、封装安全载荷(Encapsulating Security Payload，ESP)协议、密钥管理(Internet Key Exchange，IKE)协议和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议，确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

1. 认证报头协议

认证报头(Authentication Header，AH)协议为 IP 通信提供数据源认证、数据完整性和反重播保证，它能保护通信免受篡改，但不能防止窃听，适用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报头。此报头包含一个带密钥的 Hash 散列，可以将其当作数字签名，但它不使用证书，此 Hash 散列在整个数据包中计算，因此对数据的任何更改将致使散列无效，这样就提供了完整性保护。但是 AH 不提供保密服务。IPSec 支持的认证算法有 HMAC-MD5、HMAC-SHA1。

2. 封装安全载荷协议

封装安全载荷(Encapsulating Security Payload，ESP)协议为 IP 数据包提供完整性检查、认证和加密，它提供机密性并可防止窜改。ESP 服务依据建立的安全关联(SA)是可选的，然而也有一些限制，它必须与完整性检查和认证一起进行。仅当与完整性检查和认证一起进行时，重播(Replay)保护才是可选的。重播保护只能由接收方选择。

ESP 的加密服务是可选的，但如果启用加密，则也就同时选择了完整性检查和认证。因为如果仅使用加密，入侵者就可能伪造报文以发动密码分析攻击。

ESP 可以单独使用，也可以和 AH 结合使用。一般 ESP 不对整个数据包加密，而是只加密 IP 包的有效载荷部分，不包括 IP 头。但在端对端的隧道通信中，ESP 需要对整个数据包加密。ESP 报头插在 IP 报头之后，TCP 或 UDP 等传输层协议报头之前。ESP 由 IP 协议号 50 标识。

3. 密钥管理协议

密钥管理(Internet Key Exchange，IKE)协议是 Internet 工程任务组(IETF)制定的安全关联标准法和密钥交换解决方案，它提供一种方法供两台计算机建立安全关联(Security Association，SA)。SA 对两台计算机之间的策略协议进行编码，指定它们将使用哪些算法和什么样的密钥长度，以及实际的密钥本身。IKE 主要完成两个任务：安全关联的集中化管理，减少连接时间；密钥的生成和管理。

4. 实现方式

IPSec 可以在端系统或者安全网关中实现，也可以在现有的 IP 实现中集成 IPSec，这种方法需要能够修改现有 IP 实现的源码；BITS(Bump In The Stack)实现方式是在已有的 IP 协议栈中实现 IPSec，使之存在于 IP 协议和网络驱动器之间；BITW(Bump In The Wire)实现方式是在外部的加密机中实现 IPSec，从而在两个路由器或两个主机之间形成安全隧道。

IPSec 的一个重要实现方式是基于 VPN(Visual Private Network)的加密机制，由 IPSec 构成的加密 IP 隧道，提供了不同介质和地域网间的安全透明连接。

8.8.1.4 安全套接层协议

安全套接层(Secure Socket Layer，SSL)协议是 Netscape 公司设计的主要用于 Web 的安全传输协议。这种协议在 Web 上获得了广泛的应用。

SSL 是介于 HTTP 与 TCP 之间的可选层。当发送访问请求时，在 SSL 层，借助下层协议的信道安全协商出一份加密密钥，并用此密钥来加密 HTTP 请求。在 TCP 层，与服务器端口建立连接，传递 SSL 处理后的数据。接收端与此过程相反。这样，SSL 在 TCP 之上建立了一个加密通道，通过这一层的数据经过了加密，因此达到保密的效果。

SSL 协议分为两部分：握手协议(Handshake Protocol)和记录协议(Record Protocol)。其中握手协议用来协商密钥，协议的大部分内容就是通信双方如何利用它来安全地协商出一份密钥；记录协议则定义了传输的格式。

1. 握手协议

握手协议是 SSL 的客户端，也是 TCP 的客户端，在 TCP 连接建立之后，发出一个 Clienthello 来发起握手，这个消息中包含了客户端自己可实现的算法列表和其他一些需要的消息；SSL 的服务器端会回应一个 Serverhello，其中确定了通信所需要的算法，然后发过去自己的证书，里面包含了身份和自己的公钥。客户端在收到这个消息后会生成一个秘密消息，用 SSL 服务器的公钥加密后传过去，SSL 服务器端用自己的私钥解密后，会话密钥协商成功，双方可以用同一份会话密钥进行通信。

例如，一个用户通过浏览器访问 SSL 的 Web 服务器的过程如下。

(1) 浏览器和 Web 服务器开始建立一次 SSL 握手：双方协商使用的加密算法；浏览器端验证 Web 服务器提交的证书；双方协商生成会话密钥。

(2) Web 服务器向浏览器发送所请求的数据：Web 服务器计算原始数据的散列值；用会话密钥加密散列值；将密文发送给浏览器。

(3) 浏览器接收处理并显示数据：用会话密钥解密得到原始数据和散列值；使用相同的散列函数计算散列值；比较收到的散列值和计算出的散列值，如果相同则显示数据。

2. 记录协议

SSL 记录协议是一个可相对独立工作的协议。记录协议定义了传输的格式，其报文包含长度、描述符和用户数据等内容。记录协议完成的工作包括信息传输、数据分段、可选择的数据压缩、提供信息鉴别码和加密。

SSL 记录层从上层接收任意长的用户数据，然后进行合适的分段，之后再使用压缩状态信息来压缩和解压缩记录。记录的另一个功能是负载保护，就是加密和完整性保护。

3. 传输层安全性

IETF 将 SSL 作了标准化，标准文献是 RFC 2246，并将其称为传输层安全性(Transport Layer Security，TLS)。从技术上讲，TLS 与 SSL 的差别非常微小。TLS 提供了客户机与服务器之间的安全连接。TLS 协议运行于 TCP/IP 之上，在高层协议(如 HTTP)之下，因此它可以为高层协议数据提供机密性。安全连接所提供的信任、机密性和性能的级别各有不同，并且都取决于客户机和服务器的 TLS 配置。

8.8.2 典型例题分析

例 8-20 IPSec 用于增强 IP 网络的安全性，下面的说法中不正确的是 (39) 。(2017 年上半年真题 39)

A. IPSec 可对数据进行完整性保护

B. IPSec 提供用户身份认证服务

C. IPSec 的认证头添加在 TCP 封装内部

D. IPSec 对数据加密传输

解析： 在传输模式下，IPSec 包头添加在原 IP 包头和数据之间，在整个传输层报文段的后面和签名处添加一些控制字段，构成 IPSec 数据报。隧道模式是对整个 IP 数据包提供安全传输机制，是在一个 IP 数据包的前面和后面都添加一些控制字段从而形成 IPSec 数据报。

答案： C

8.8.3 同步练习

1. 以下关于 IPSec 协议的描述中，正确的是________。
   A. IPsec 认证报头(AH)不提供数据加密服务
   B. IPsec 封装安全载荷(ESP)用于数据完整性认证和数据源认证
   C. IPsec 的传输模式对原来的 IP 数据报进行了封装和加密，再加上了新的 IP 头
   D. IPsec 通过应用层的 Web 服务监理安全连接
2. 下列隧道协议中工作在网络层的是________。
   A. SSL B. L2TP C. IPSec D. PPTP
3. HTTPS 采用________协议实现安全网站访问。
   A. SSL B. IPSec C. PGP D. SET
4. IPSec 的加密和认证过程中所使用的密钥由________机制来生成和分发。
   A. ESP B. IKE C. TGS D. AH

8.8.4 同步练习参考答案

1. A 2. C 3. A 4. B

8.9 应用层安全协议

8.9.1 考点辅导

8.9.1.1 S-HTTP

安全超文本传输协议(Secure Hyper Text Transfer Protocol，S-HTTP)是一种结合 HTTP 而设计的消息的安全通信协议。S-HTTP 的设计基于与 HTTP 信息样板共存并易于与 HTTP

应用程序整合。

S-HTTP 协议为 HTTP 客户机和服务器提供了多种安全机制，这些安全服务选项是适用于万维网上各类用户的，还为客户机和服务器提供了对称能力(及时处理请求和回复，及两者的参数选择)，同时维持 HTTP 的通信模型和实施特征。

S-HTTP 不需要客户方的公用密钥证明(或公用密钥)，但它支持对称密钥的操作模式。这一点很重要，因为这意味着在没有要求用户个人建立公用密钥的情况下，会自发地发生私人交易。它支持端对端安全传输，客户机可能首先启动安全传输(使用报头的信息)，用来支持加密技术。

在语法上，S-HTTP 报文与 HTTP 相同，由请求或状态行组成，后面是信头和主体。请求报文的格式由请求行、通用信息头、请求头、实体头、信息主体组成。响应报文由响应行、通用信息头、响应头、实体头、信息主体组成。

8.9.1.2 PGP

PGP(Pretty Good Privacy)是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术。PGP 并没有使用什么新的概念，它只是将现有的一些算法如 MD5、RSA 及 IDEA 等综合在一起。PGP 提供数据加密和数字签名两种服务。图 8-11 所示为 PGP 的加密过程。

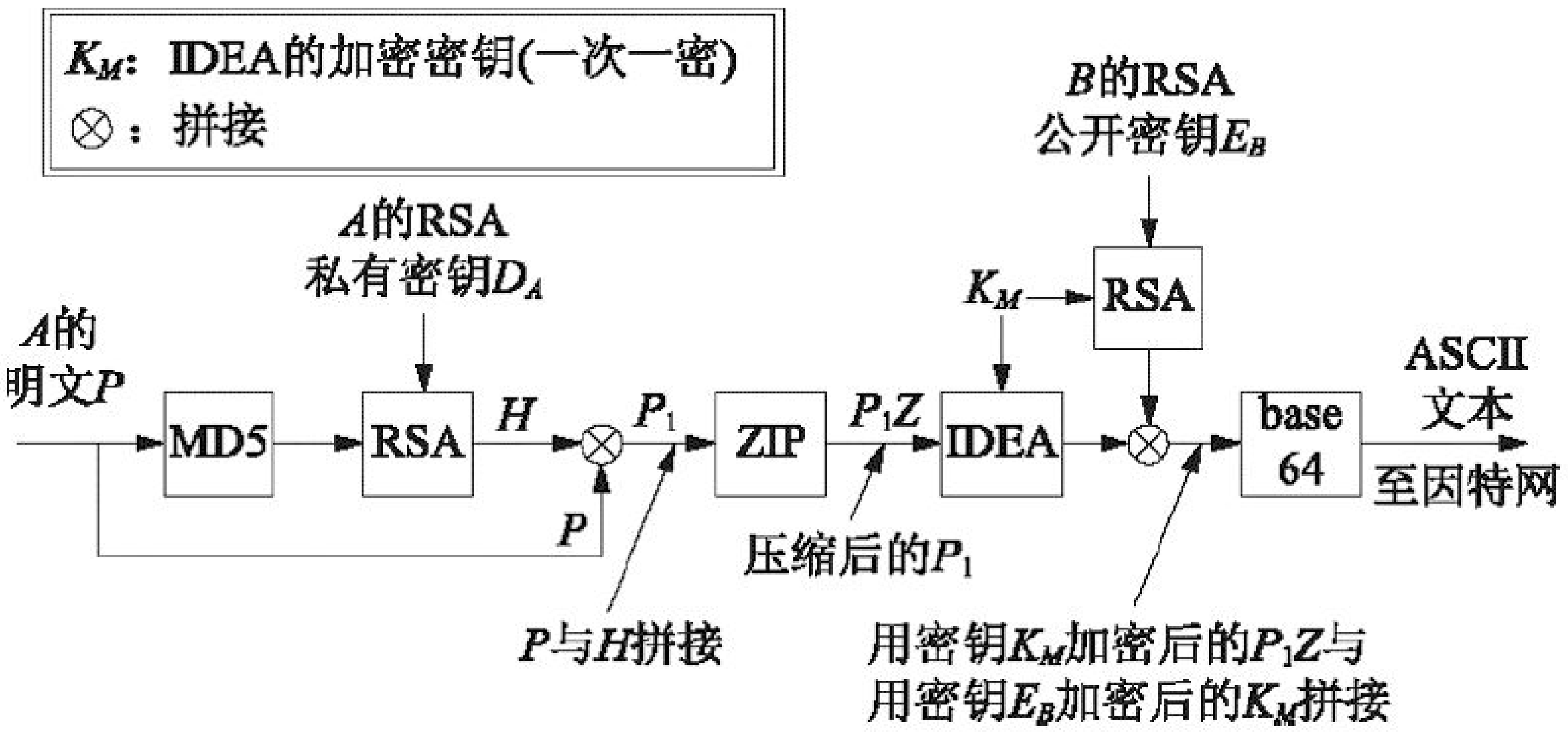


图 8-11 PGP 加密过程

数字加密机制可以应用于本地存储文件，也可以应用于网络上传输的电子邮件。数字签名机制用于数据源身份认证和报文完整性验证。PGP 使用 RSA 公钥证书进行身份认证，使用 IDEA(128 位密钥)进行数据加密，使用 MD5 进行数据完整性认证。

8.9.1.3 S/MIME

S/MIME(Security/Multipurpose Internet Mail Extensions)是 RSA 数据安全公司开发的软件。S/MIME 提供的安全服务有报文完整性验证、数字签名和数据加密。S/MIME 可以添加在邮件系统的用户代理中，用于提供安全的电子邮件传输服务，也可以加入其他的传输机制中，安全地传输任何 MIME 报文，甚至可以添加在自动报文传输代理中，在 Internet 中安全地传送由软件生成的 FAX 报文。

S/MIME 的安全功能基于加密信息语法标准 PKCS#7(RFC2315)和 X.509v3 证书，密钥长度是动态可变的，具有很高的灵活性。

8.9.1.4　安全的电子交易

安全的电子交易(Secure Electronic Transaction，SET)用于电子商务的行业规范，是一种应用在 Internet 上、以信用卡为基础的电子付款系统规范，目的是保证网络交易的安全。SET 主要使用“电子认证”技术作为保密电子交易安全进行的基础，其认证过程使用 RSA 和 DES 算法。

1. SET 提供的服务

SET 提供以下 3 种服务。

(1) 在交易涉及的双方之间提供安全信道。

(2) 使用 X.509 数字证书实现安全的电子交易。

(3) 保证信息的机密性。

2. SET 交易过程

SET 交易发生的先决条件是，每一个持卡人(客户)必须拥有一个唯一的电子(数字)证书，且由客户确定口令，并用这个口令对数字证书、私钥、信用卡号码及其他信息进行加密存储，这些与符合 SET 协议的软件一起组成了一个 SET“电子钱包”。图 8-12 展示了 SET 交易过程中，持卡人、商家、支付网关、收单银行和发卡机构之间的数据交换过程。

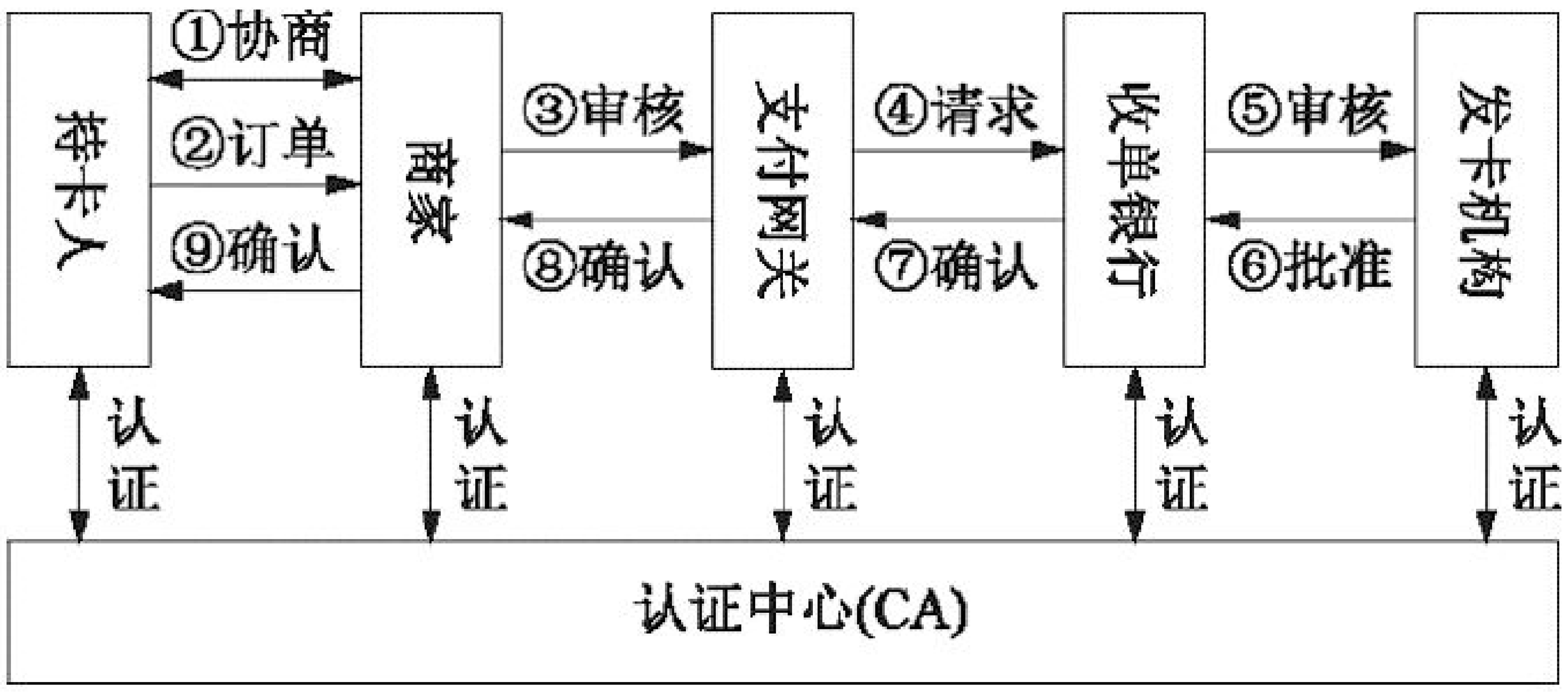


图 8-12　SET 交易过程

8.9.1.5　Kerberos

Kerberos 是 MIT 为校园网用户访问服务器进行身份认证而设计的安全协议，它可以防止偷听和重放攻击，保护数据的完整性。

Kerberos 系统为分布式计算环境提供了一种对用户双方进行验证的认证方法。它使网络上进行通信的用户相互证明自己的身份，同时又可选择防止窃听或中继攻击。它的安全机制在于首先对发出请求的用户进行身份验证，确认其是否为合法用户，若是合法用户则再审核该用户是否有权利对其所请求的服务器或主机进行访问。从加密算法上来讲，其验证是建立在对称加密(DES)的基础上的，它采用可信任的第三方——密钥分配中心(KDC)保存与所有密钥持有者通信的主密钥(秘密密钥)。

Kerberos 的目标在于 3 个领域：认证、授权和记账审计。认证过程如图 8-13 所示。

(1) 用户向 KDC 申请初始票据。

(2) KDC 向用户发放 TGT 会话票据。

(3) 用户向 TGS 请求会话票据。

(4) TGS 验证用户身份后发放给用户会话票据 K_{AV}。

(5) 用户向应用服务器请求登录。

(6) 应用服务器向用户验证时间戳。

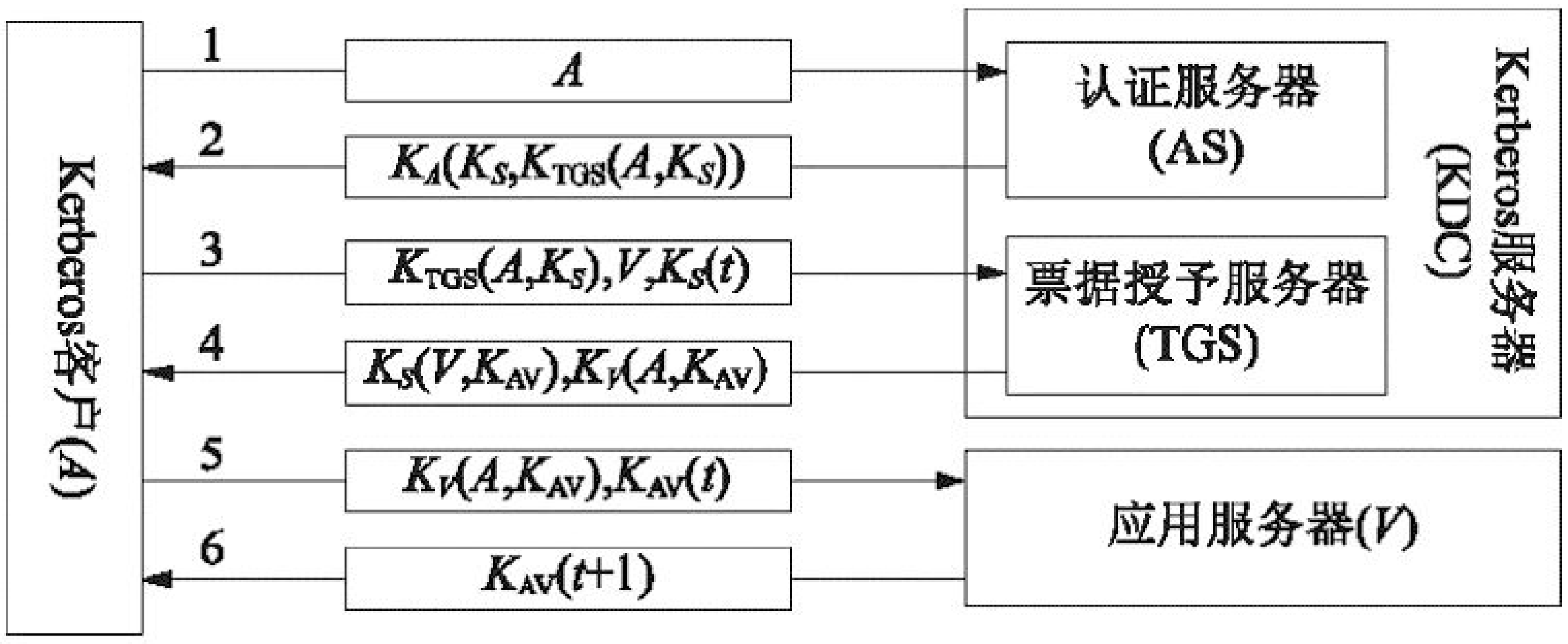


图 8-13 Kerberos 的认证过程

8.9.2 典型例题分析

例 8-21 下列__(44)__不能提供应用层安全。(2015 年下半年真题 44)

A. S-HTTP　　B. PGP　　C. MIME　　D. SET

解析：本题考查应用层安全协议的基础知识。

以上 4 个选项中，S-HTTP 是安全的 HTTP，采用了超文本信息的协议，一般用于安全性要求较高的 Web 浏览环境，如电子商务网页浏览、通过网页支付等环境，它提供的是应用层的安全服务。HTTPS 是经过 SSL 加密的。

PGP 是传输安全电子邮件的协议，可对电子邮件进行加密、签名等操作，它提供的是应用层安全服务。

MIME (Multipurpose Internet Mail Extensions，多用途互联网邮件扩展类型)是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。它并未提供任何应用层安全服务。

SET (Secure Electronic Transaction，简称 SET 协议)主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的，以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份，以及可操作性。SET 中的核心技术主要有公开密钥加密、数字签名、电子信封、安全证书等，它提供的是应用层安全服务。

答案：C

例 8-22 提供电子邮件安全服务的协议是__(39)__。(2015 年上半年真题 39)

A. PGP　　B. SET　　C. S-HTTP　　D. Kerberos

解析：PGP(Pretty Good Privacy)，是一个基于 RSA 公钥加密体系的邮件加密协议，可以用它对邮件进行保密以防止非授权者阅读，它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者，并能确信邮件没有被窜改。

答案：A

8.9.3　同步练习

1.　PGP(Pretty Good Privacy)是一种电子邮件加密软件包，它提供数据加密和数字签名两种服务，采用__(1)__进行身份认证，使用__(2)__(128 位密钥)进行数据加密，使用__(3)__进行数据完整性验证。

(1) A. RSA 公钥证书　B. RSA 私钥证书　C. Kerboros 证书　D. DES 私钥证书

(2) A. IDEA　B. RSA　C. DES　D. Diffie-Hellman

(3) A. Hash　B. MDS　C. 三重 DES　D. SHA-1

2.　以下关于 S-HTTP 的描述中，正确的是________。

A. S-HTTP 是一种面向报文的安全通信协议，使用 TCP 443 端口

B. S-HTTP 所使用的语法和报文格式与 HTTP 相同

C. S-HTTP 也可以写为 HTTPS

D. S-HTTP 的安全基础并非 SSL

8.9.4　同步练习参考答案

1. (1) A　(2) A　(3) B　　2. D

8.10　可信任系统

8.10.1　考点辅导

通常将可信任系统定义为：一个由完整的硬件及软件所组成的系统，在不违反访问权限的情况下，它能同时服务于不限定个数的用户，并处理从一般机密到最高机密等不同范围的信息。

更进一步，将一个计算机系统可接受的信任程度加以分级，凡符合某些安全条件、基准、规则的系统即可归类为某种安全等级。将计算机系统的安全性能由高到低划分为 A、B、C、D 共 4 个大等级 7 个小等级，特别是较高等级的安全范围涵盖较低等级的安全范围，而每个大等级又以安全性高低依次编号细分成数个小等级。

1. D 级，最低保护(Minimal Protection)

D 级也称安全保护欠缺级，凡没有通过其他安全等级测试项目的系统即属于该级，如 IBM-PC、Apple Macintosh 等个人计算机的系统虽未经安全测试，但如果有，很可能属于此级。D 级并非没有安全保护功能，只是太弱。

2. C 级，自定式保护(Discretionary Protection)

C 级的安全特点在于系统的对象(如文件、目录)可由系统的主体(如系统管理员、用户、

应用程序)自定义访问权限，如管理员可以决定某个文件仅允许一特定用户读取、另一用户写入，某人可以决定他的某个目录可公开给其他用户读、写等。在 UNIX、Windows NT 等操作系统都可以见到这种属性。该等级又按安全低、高分为 C1、C2 两个安全等级。

1) C1 级，自主安全保护级

可信计算基(Trusted Computing Base，TCB)定义和控制系统中命名用户对命名客体的访问。实施机制(如访问控制表)允许命名用户和(或)用户组的身份规定并控制客体的共享，阻止非授权用户读取敏感信息。

可信计算基是指为实现计算机处理系统安全保护策略的各种安全保护机制的集合。

2) C2 级，受控存取保护级

与自主安全保护级相比，本级的可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件及隔离资源，使用户能对自己的行为负责。

3. B 级，强制式保护(Mandatory Protection)

B 级的安全特点在于由系统强制的安全保护，在强制式保护模式中，每个系统对象(如文件、目录等资源)及主体(如系统管理员、用户、应用程序)都有自己的安全标签(Security Label)，系统即依据用户的安全等级赋予其对各对象的访问权限。

1) B1 级，标记安全保护级

本级的可信计算基具有受近期存取保护级的所有功能。此外，还可提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；可消除通过测试发现的任何错误。

2) B2 级，结构化保护级

本级的可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将 B1 级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的可信计算基必须结构化为关键保护元素和非关键保护元素。可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了认证机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当强的抗渗透能力。

3) B3 级，安全域级

本级的可信计算基满足访问监控器需求。访问监控器是指监控主体和客体之间授权访问关系的部件。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的，必须足够小，能够分析和测试。为了满足访问监控器需求，可信计算基在其构造时排除实施对安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最低程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

4. A 级，可验证保护(Verified Protection)

虽然橘皮书仍可能定义比 A1 高的安全等级，但目前此级仅有 A1 等级，A 等级的功能基本上与 B3 级的相同，其特点在于 A 等级的系统拥有正式的分析及数学方法可完全证明该系统的安全策略及安全规格的完整性与一致性。本级还规定了将安全计算机系统运送

到现场安装所必须遵守的程序。

可信任计算机系统评量基准(Trusted Computer System Evaluation Criteria)是美国国家安全局(NSA)的国家计算机安全中心(NCSC)于 1983 年 8 月颁发的官方标准，是目前颇具权威的计算机系统安全标准之一。例如，微软 Windows NT 4.0 及以上版本目前具有 C2 安全等级。也就是说，它的安全特性就是在于自定式保护，NT 未来可能提高到 B2 安全等级。Windows 2000 已顺利获得认证。UNIX 未经测试时，一般认为是 C1，也有人认为是 C2。

8.10.2　典型例题分析

例 8-23　最低的保护级是________。

A. A 级　　B. B 级　　C. C 级　　D. D 级

解析：D 级也称安全保护欠缺级，凡没有通过其他安全等级测试项目的系统即属于该级。

答案：D

8.10.3　同步练习

下列不是 B 级(强制式保护)的是________。

A. B1　　B. B2　　C. B3　　D. B4

8.10.4　同步练习参考答案

D

8.11　防　火　墙

8.11.1　考点辅导

8.11.1.1　防火墙的概念

防火墙一词来自建筑物中的同名机构，从字面意思上说，它可以防止火灾从建筑物的一部分蔓延到其他部分。Internet 防火墙也要起到同样的作用，防止 Internet 上的不安全因素蔓延到自己企业或组织的内部网。防火墙技术早在 1994 年就被 RFC 1636 列为信息系统安全机制不可缺少的一项措施。

从狭义上说，防火墙是指安装了防火墙软件的主机或路由器系统；从广义上说，防火墙还包括整个网络的安全策略和安全行为。

AT&T 的两位工程师 William Cheswich 和 Steven Bellovin 给出了防火墙的明确定义：所有的从外部到内部或从内部到外部的通信都必须经过它；只有有内部访问策略授权的通

信才能被允许通过；系统本身具有很强的高可靠性。

总之，防火墙是一种网络安全保障手段，是网络通信时执行的一种访问控制尺度，其主要目标就是通过控制入、出一个网络的权限，并迫使所有的连接都经过这样的检查，防止一个需要保护的网络遭受外界因素的干扰和破坏。在逻辑上，防火墙是一个分离器、一个限制器，也是一个分析器，可有效地监视内部网络和 Internet 之间的任何活动，保证内部网络的安全；在物理实现上，防火墙是位于网络特殊位置的一组硬件设备——路由器、计算机或其他特制的硬件设备。防火墙可以是一个独立的系统，也可以在一个进行网络互联的路由器上实现防火墙。

防火墙的发展共经历了以下 4 个阶段。

(1) 基于路由器的防火墙阶段。

(2) 用户化的防火墙工具套阶段。

(3) 建立在通用操作系统上的防火墙阶段。

(4) 具有安全操作系统的防火墙阶段。

8.11.1.2 防火墙的基本类型

防火墙的基本类型如下。

(1) 包过滤型防火墙。通过访问控制表，检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，来确定是否允许该数据包通过。

(2) 应用网关防火墙。它工作在应用层，能针对特别的网络应用协议制定数据过滤规则。

(3) 代理服务器防火墙。它工作在 OSI 模型的应用层，主要使用代理技术来阻断内部网络和外部网络之间的通信，达到隐藏内部网络的目的。

(4) 状态检测防火墙。也叫自适应防火墙或动态包过滤防火墙。这种防火墙能通过状态检测技术动态记录、维护各个连接的协议状态，并且在网络层和 IP 之间插入一个检查模块，对 IP 包的信息进行分析检测，以决定是否允许通过防火墙。

(5) 自适应代理防火墙。根据用户的安全策略，动态适应传输中的分组流量。它整合了动态包过滤防火墙技术和应用代理技术，本质上是状态检测防火墙。

8.11.1.3 防火墙的设计

1. 设计原则

防火墙的设计原则如下。

(1) 由内到外、由外到内的业务流均要经过防火墙。

(2) 只允许本地安全策略认可的业务流通过防火墙，实行默认拒绝原则。

(3) 严格限制外部网络的用户进入内部网络。

(4) 具有透明性，方便内部网络用户，保证正常的信息通过。

(5) 具有抗穿透攻击能力，强化记录、审计和报警。

2. 基本组成

防火墙主要包括以下 5 个部分：安全操作系统、过滤器、网关、域名服务、函件处理。

(1) 安全操作系统。防火墙本身必须建立在安全操作系统中，由安全操作系统来保护防火墙的源代码和文件免遭入侵者的攻击。

(2) 过滤器。外部过滤器保护网关不受攻击，内部过滤器在网关被攻破后提供对内部网络的保护。

(3) 网关。提供中继服务，辅助过滤器控制业务流。可以在其上执行一些特定的应用程序或服务器程序，这些程序统称为“代理程序”。

(4) 域名服务。将内部网络的域名和 Internet 相隔离，使内部网络中主机的 IP 地址不至于暴露给 Internet 中的用户。

(5) 函件处理。保证内部网络用户和 Internet 用户之间的任何函件交换都必须经过防火墙处理。

8.11.1.4 防火墙的功能和网络拓扑结构

防火墙的功能和网络拓扑结构如下。

(1) 屏蔽路由器结构。通常由过滤路由器实现，也可以用主机来实现。屏蔽路由器作为内外连接的唯一通道，要求所有的报文都必须在此通过检查。

(2) 双穴主机结构。双穴主机具有两个网络接口，它的位置位于内部网络与 Internet 的连接处，运行应用代理程序，充当内、外网络之间的转发器，如图 8-14 所示。

(3) 屏蔽主机结构。由屏蔽路由器与堡垒主机构成，屏蔽路由器位于内部网络与 Internet 之间的连接处，而堡垒主机位于内部网络，如图 8-15 所示。

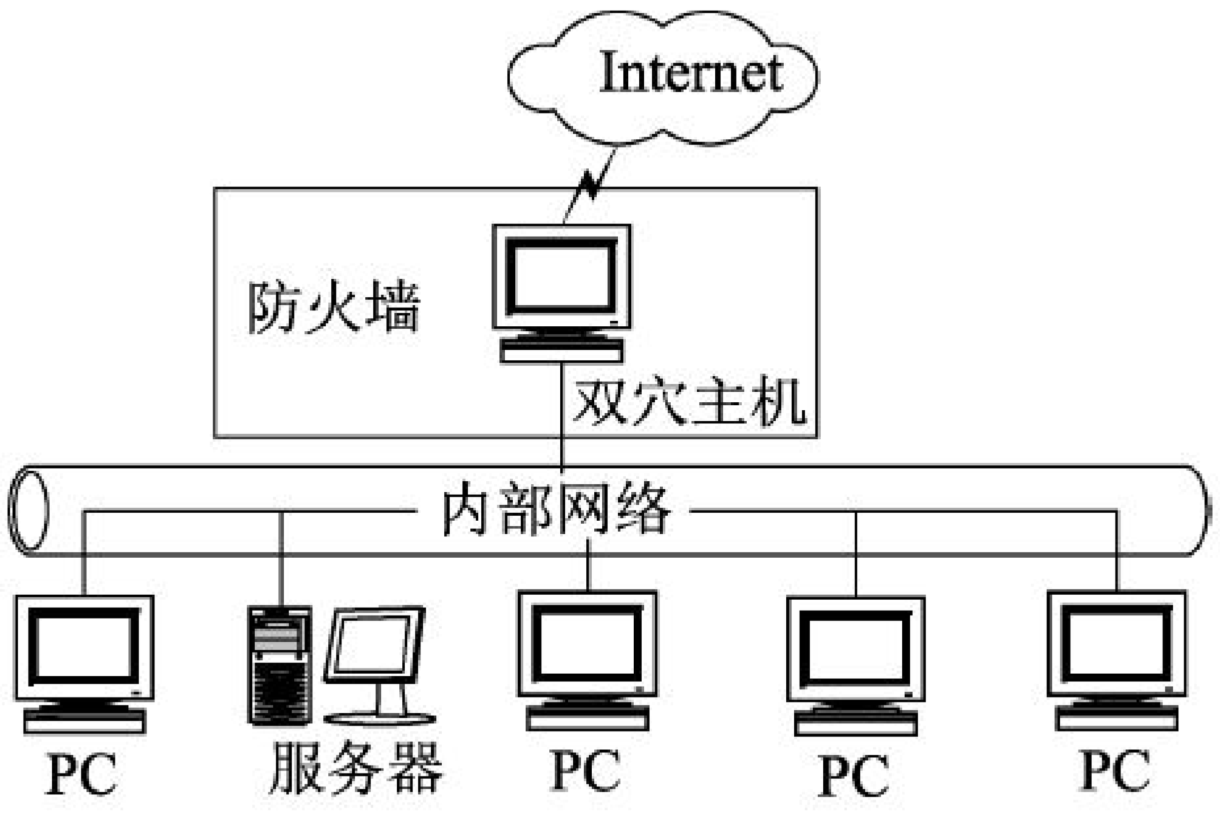


图 8-14 双穴主机结构

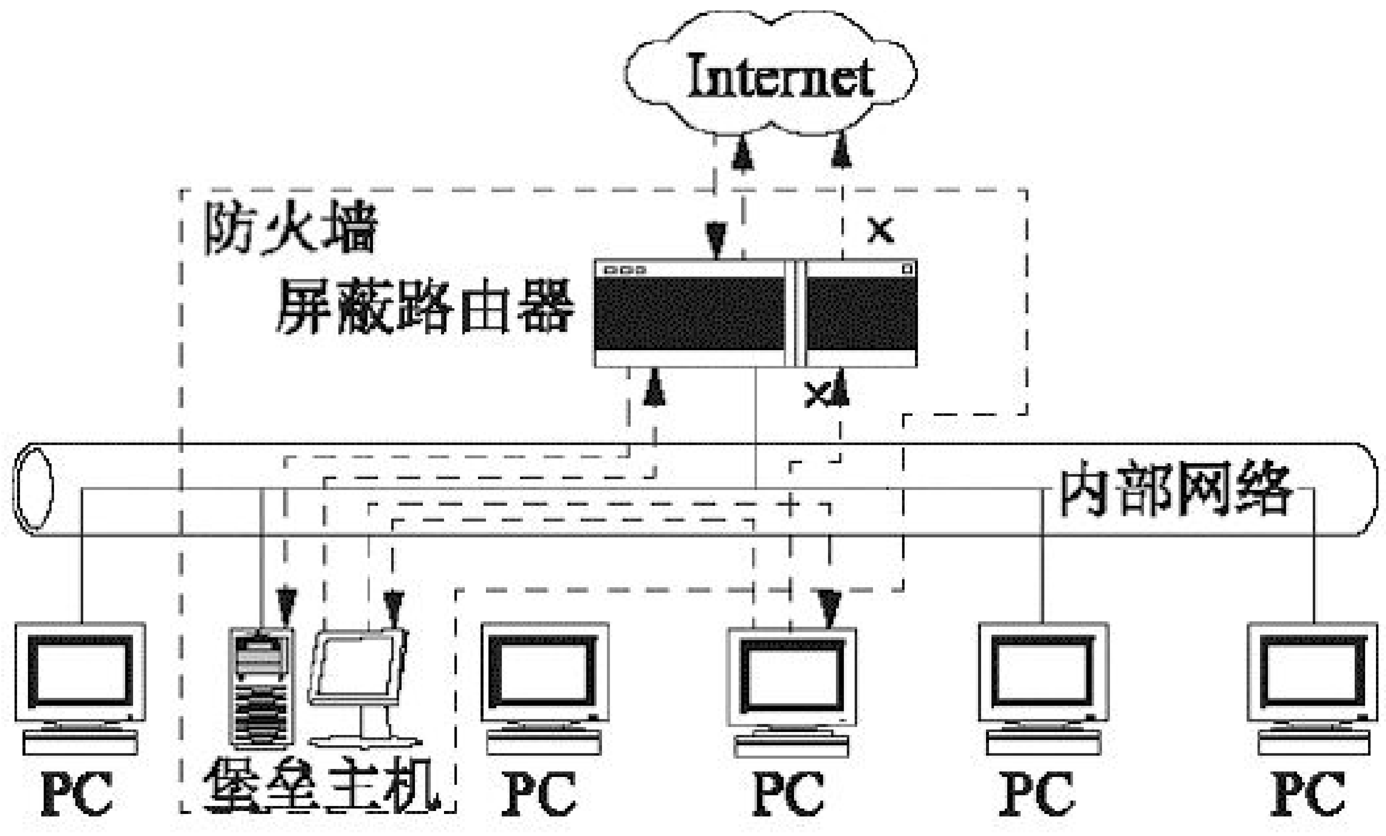


图 8-15 屏蔽主机结构

(4) 屏蔽子网结构。在屏蔽主机结构的基础上增加了一个周边防御网段，用以进一步隔离内部网络与外部网络，如图 8-16 所示。

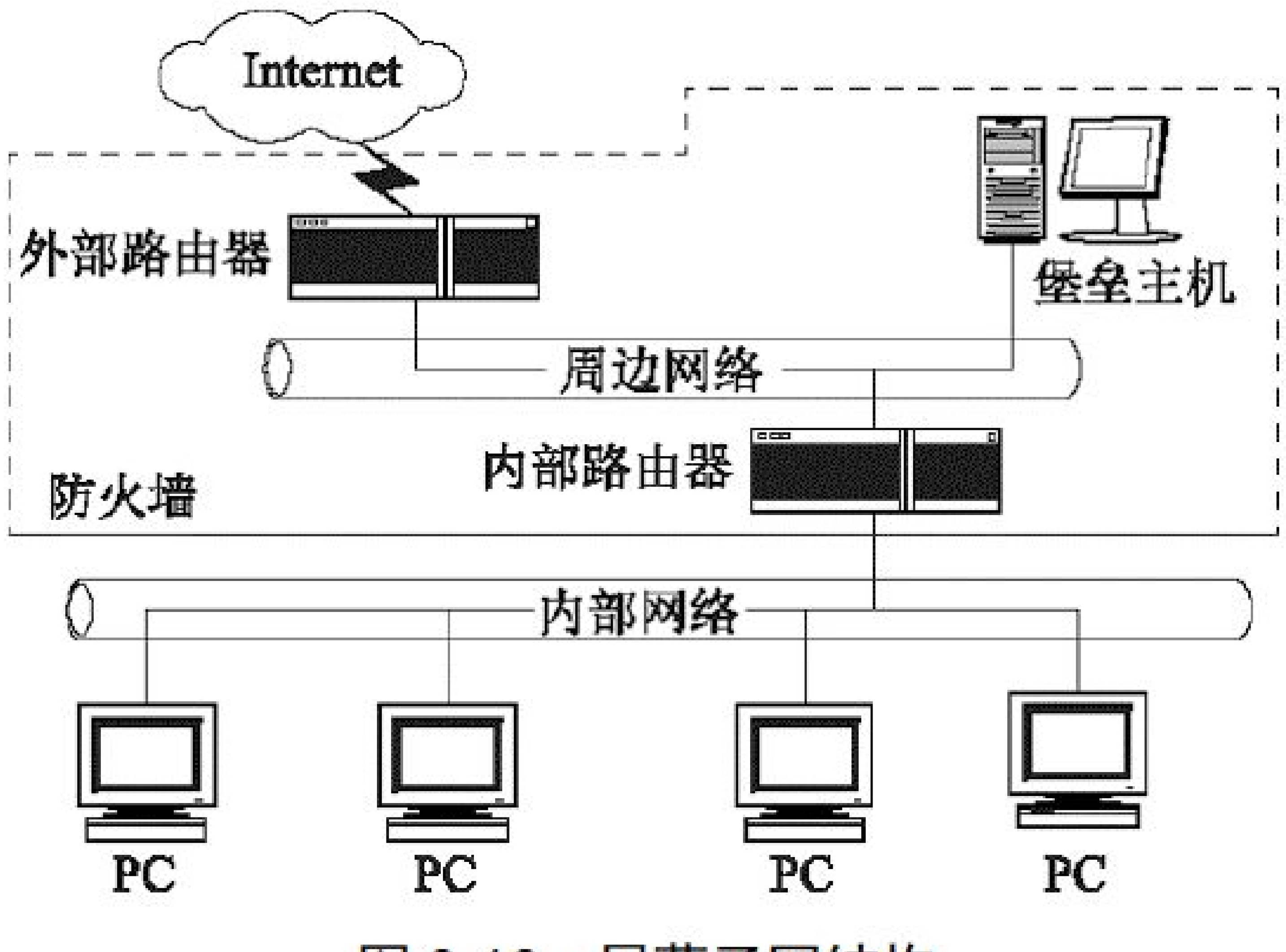


图 8-16 屏蔽子网结构

周边防御网段是位于内部网络与外部网络之间的另一层安全网段，分别由内、外两个屏蔽路由器与其相连。周边防御网段所构成的安全子网又称为“非军事区”(DeMilitrized Zone，DMZ)，这一网段受到安全威胁不会影响到内部网络。DMZ 是放置公共信息的最佳位置，通常把 WWW、FTP、电子邮件、电子商务等服务器都存放在该区域。而把内部服务器、个人 PC 等应用放置在内网中。

8.11.2 典型例题分析

例 8-24 防火墙不具备__(45)__功能。(2015 年下半年真题 45)

A. 包过滤　　B. 查毒　　C. 记录访问过程　　D. 代理

解析：具体来说，防火墙主要有以下几方面功能。

(1) 创建一个检查点。防火墙在一个公司内部网络和外部网络间建立一个检查点。这种实现要求所有的流量都要通过这个检查点。一旦这些检查点清楚地建立，防火墙设备就可以监视、过滤和检查所有进来和出去的流量。

(2) 隔离不同网络，防止内部信息的外泄。这是防火墙的最基本功能，它通过隔离内、外部网络来确保内部网络的安全，也限制了局部重点或敏感网络安全问题对全局网络造成的影响。

(3) 强化网络安全策略。通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更方便，更能有效地对网络安全性能起到加强作用。

(4) 有效地审计和记录内、外部网络上的活动。防火墙可以对内、外部网络存取和访问进行监控审计。如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并进行日志记录，同时也能提供网络使用情况的统计数据。

答案：B

例 8-25 下列关于防火墙的设计原则，说法错误的是________。

A. 由内到外、由外到内的业务流均要经过防火墙

B. 只允许本地安全策略认可的业务流通过防火墙，实行默认拒绝原则

C. 严格限制外部网络的用户进入内部网络

D. 具有不透明性

解析：防火墙的设计原则：具有透明性，方便内部网络用户，保证正常的信息通过。

答案：D

8.11.3 同步练习

1. 防火墙的工作层次是决定防火墙的工作效率及安全性的主要因素，下面的叙述中正确的是________。

A. 防火墙工作层次越低，工作效率越高，安全性越高

B. 防火墙工作层次越低，工作效率越低，安全性越低

C. 防火墙工作层次越高，工作效率越高，安全性越低

D. 防火墙工作层次越高，工作效率越低，安全性越高

2. 防火墙的发展共经历了 4 个阶段，下列说法错误的是________。

A. 基于交换机的防火墙阶段　　B. 用户化的防火墙工具套阶段

C. 建立在通用操作系统上的防火墙阶段　D. 具有安全操作系统的防火墙阶段

3. 包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的检查内容一般不包括______。

A. 源地址　　B. 目的地址　　C. 协议　　D. 有效载荷

8.11.4　同步练习参考答案

1.D　2. A　3. D

8.12　病 毒 防 护

8.12.1　考点辅导

1. 病毒的定义

按照《中华人民共和国计算机信息系统安全保护条例》中的规定，计算机病毒指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

在病毒的生存期内，典型的病毒经历了下面 4 个阶段。

(1) 潜伏阶段。

(2) 繁殖阶段。

(3) 出发阶段。

(4) 执行阶段。

2. 病毒的分类

对于最重要的病毒类型，建议如下的分类方法。

(1) 寄生病毒：将自己附加到可执行文件中，当被感染的程序执行时，找到其他可执行文件并感染。

(2) 存储器驻留病毒：寄宿在主存中，作为驻留程序的一部分；从那时起，病毒感染每个执行的程序。

(3) 引导区病毒：感染主引导记录或引导记录，并且当系统从包含病毒的磁盘启动时进行传播。

(4) 隐形病毒：能在反病毒软件检测时隐藏自己。

(5) 多形病毒：每次感染都会改变的病毒，使得不可能通过病毒的“签名”来检测自己。

3. 防病毒技术

在所有计算机安全威胁中，计算机病毒是最为严重的，它不仅发生的频率高、损失大，而且潜伏性强、覆盖面广。计算机病毒具有不可估量的威胁性和破坏力，防范病毒是网络安全技术中重要的一环。防病毒技术包括预防病毒、检测病毒、消除病毒等技术。

8.12.2 典型例题分析

例 8-26 宏病毒可以感染后缀为__(41)__的文件。(2015 年上半年真题 41)

A. exe　　B. txt　　C. pdf　　D. xls

解析：宏病毒的共同特点是能感染 Office 文档，然后通过 Office 通用模板进行传播。xls 是 Excel 文档的后缀名，Excel 是 Office 的组件之一，可以被宏病毒感染。

答案：D

8.12.3 同步练习

1. 为了防止电子邮件中的恶意代码，应该用______方式阅读电子邮件。

   A. 纯文本　　B. 网页　　C. 程序　　D. 会话

2. 计算机感染特洛伊木马后的典型现象是______。

   A. 程序异常退出　　B. 有未知程序试图建立网络连接

   C. 邮箱被垃圾邮件填满　　D. Windows 系统黑屏

8.12.4 同步练习参考答案

1. A　2. B

8.13 入 侵 检 测

8.13.1 考点辅导

8.13.1.1 入侵检测系统概述

1. 入侵检测系统的框架结构

DARPA 提出的公共入侵检测框架(CIDF)由 4 个模块组成：事件产生器、事件分析器、事件数据库和响应单元，如图 8-17 所示。

(1) 事件产生器(Event generators，E-boxes)。负责数据的采集，并将收集到的原始数据转换为事件，向系统的其他模块提供与事件有关的信息。入侵检测所利用的信息一般来自 4 个方面：系统和网络的日志文件、目录和文件中不期望的改变、程序执行中不期望的行为、

物理形式的入侵信息。入侵检测要在网络中的若干关键点(不同网段和不同主机)收集信息，并通过多个采集点信息的比较来判断是否存在可疑迹象或发生入侵行为。

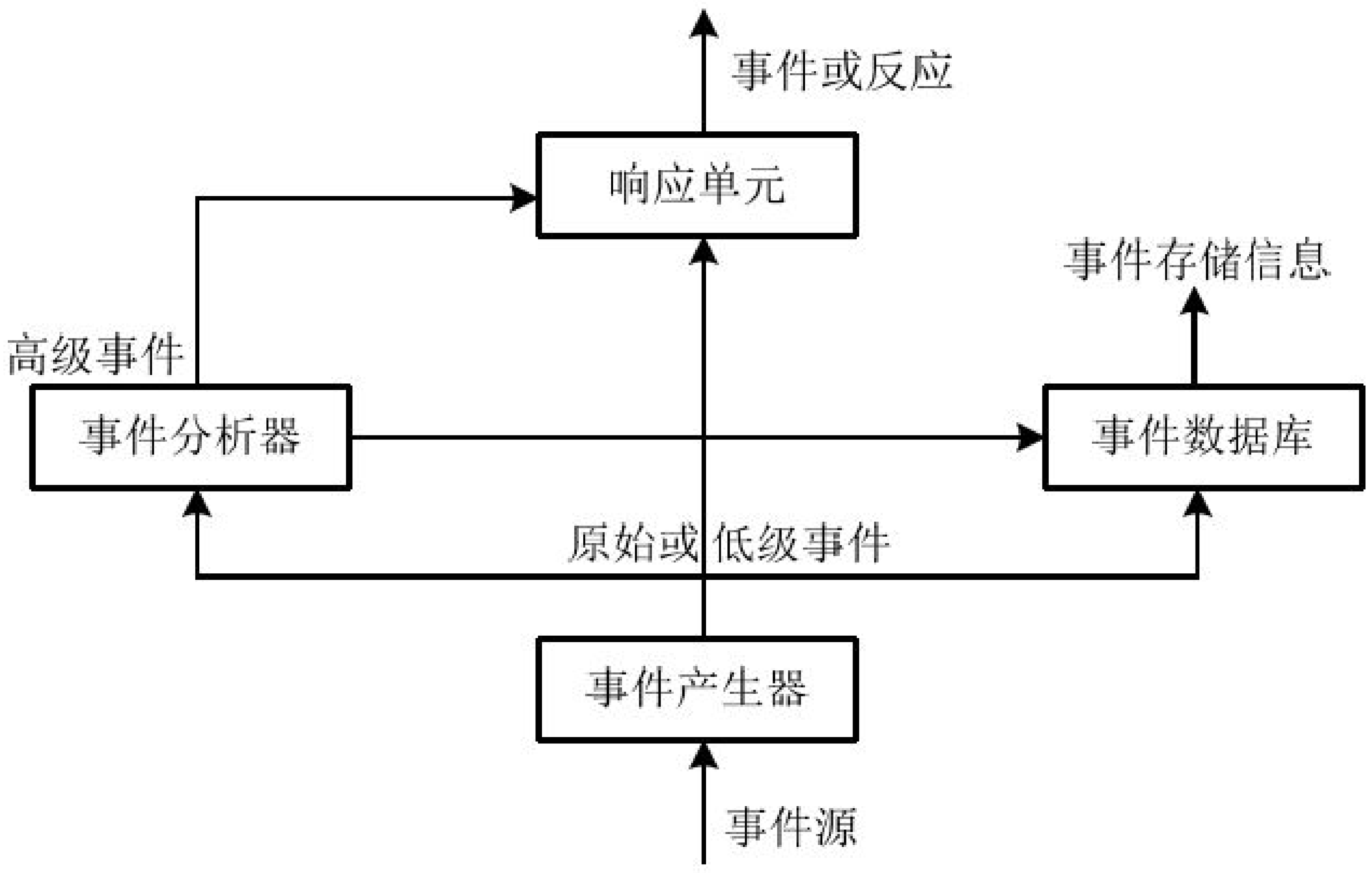


图 8-17　CIDF 体系结构

(2) 事件分析器(Event Analyzers，A-boxes)。接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，分析方法有下面 3 种。

① 模式匹配。将收集到的信息与已知的网络入侵数据库进行比较，从而发现违背安全策略的行为。

② 统计分析。首先给系统对象(例如用户、文件、目录和设备等)建立正常使用时的特征文件(Profile)，这些特征值将被用来与网络中发生的行为进行比较。当观察值超出正常值范围时，就认为有可能发生入侵行为。

③ 数据完整性分析。主要关注文件或系统对象的属性是否被修改，这种方法往往用于事后的审计分析。

(3) 事件数据库(Event Databases，D-boxes)。存放有关事件的各种中间结果和最终数据的地方，可以是面向对象的数据库，也可以是一个文本文件。

(4) 响应单元(Response units，R-boxes)。根据报警信息做出各种反应，强烈的反应就是断开连接、改变文件属性等，简单的反应就是发出系统提示，引起操作人员注意。

2. 入侵检测系统的部署位置

入侵检测系统是一个监听设备，无须跨接在任何链路上，不产生任何网络流量便可以工作。因此，对 IDS 部署的唯一要求是应当挂接在所关注流量必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量以及需要统计、监视的网络报文。目前的网络都是交换式的拓扑结构，因此一般选择在尽可能靠近攻击源，或者尽可能接近受保护资源的地方，这些位置通常是：

(1) 服务器区域的交换机上。

(2) Internet 接入路由器之后的第一台交换机上。

(3) 重点保护网段的局域网交换机上。

3. 入侵检测系统的数据源

根据不同的数据源，IDS 所使用的入侵检测技术也有所不同，目前，对于入侵检测所分析的数据源有以下几种来源。

(1) 操作系统审计记录。

(2) 操作系统日志。

(3) 网络数据。

4. 入侵检测系统的分类

根据入侵检测系统的信息来源，IDS 可分为基于主机的 IDS (HIDS)、基于网络的 IDS 以及分布式的 IDS (NIDS)。

按照入侵检测系统的相应方式的不同，可以将入侵检测系统分为实时检测和非实时检测两种。

按照数据分析的技术和处理方式，可以将入侵检测系统分为异常检测、误用检测和混合检测 3 种。

5. 检测模型的性能评价指标

评价一个入侵检测系统的性能，一般从两个方面进行考量：检测的有效性和检测的速率。其中，检测的有效性是指检测结果的精度和报警的可信度，一般使用混淆矩阵来表示。如表 8-2 所示。

表 8-2　入侵检测系统性能评估矩阵

		检测结果	
		入侵行为	正常连接
实际情况	入侵行为	*a*	*b*
	正常连接	*c*	*d*

在表 8-2 中，*a* 表示一个实际为入侵行为的检测结果为入侵行为记录的数量，表明检测的结果准确的情况：*b* 表示入侵行为被认为是正常连接记录的数量：*c* 表示正常连接被检测为入侵行为记录的数量；*d* 表示正常连接被检测为正常连接记录的数量。

一般用以下几种指标来对入侵检测系统的性能进行考量和评价。

(1) 检出率，是指一个入侵行为被检出的数量在所有入侵行为中所占的百分比，使用以下公式计算：检出率=$a/(a+b)$。

(2) 虚警率，是指一个正常连接被检测为入侵行为的数量在所有正常连接中所占的百分比，使用以下公式计算：虚警率= $c/(c+d)$。

(3) 漏警率，是指一个入侵行为被检测为正常连接的数量在所有入侵行为中所占的百分比，使用以下公式计算：漏警率= $b/(a+b)$。

(4) 查准率，指在被检测为入侵攻击记录总数中实际为入侵攻击记录所占的百分比，使用以下公式计算：查准率= $a/(a+c)$。

(5) 查全率，指入侵攻击记录被正确检测为入侵攻击的数量占入侵攻击总记录数的百分比，意味着在所有的入侵攻击中，有多大的可能性能被检测识别出来，使用以下公式计算：查全率=$a/(a+b)$。

(6) 准确率，用对网络行为正确分类所占的百分比来衡量，为检测类别正确的记录数占参与检测的总记录数的百分比，使用以下公式计算：准确率= $(a+d)/(a+b+c+d)$。

8.13.1.2　入侵检测技术

目前，入侵检测技术分为异常检测和误用检测两种。

1. 异常检测

异常检测是将网络行为分为正常的网络连接和异常网络活动两种，而异常检测是把入侵行为看作是异常活动的一个子集，通过监测网络用户在网络上的行为的特征判断是否遭到了入侵。基于异常检测常用的检测方法有以下三种。

① 基于统计的异常检测方法；

② 基于聚类分析的异常检测方法；

③ 基于神经网络的异常检测方法。

2. 误用检测

误用检测技术的研究从 20 世纪 90 年代中期就开始了。它首先对已知的入侵行为的特征进行编码，用已建立入侵行为的特征数据库，在对入侵检测过程中得到的待测数据中的特征进行分析，如能够与特征数据库中的特征匹配，则判定为入侵行为。基于误用检测的常用的检测方法有以下两种。

① 专家系统检测法；

② 模式匹配检测法。

8.13.2　典型例题分析

例 8-27　以下关于入侵检测系统的描述中，正确的是 (45) 。(2017 年下半年真题 45)

A. 实现内、外网隔离与访问控制

B. 对进出网络的信息进行实时的监测与比对，及时发现攻击行为

C. 隐藏内部网络拓扑

D. 预防、检测和消除网络病毒

解析：入侵检测系统可以检测出正在发生的攻击活动，发现攻击活动的范围和后果，诊断并发现攻击者的入侵方式和地点，给出解决建议，收集并记录入侵活动的证据。

答案：B

例 8-28　 (65) 不属于入侵检测技术。(2017 年下半年真题 65)

A. 专家系统　　B. 模型检测　　C. 简单匹配　　D. 漏洞扫描

解析：入侵检测技术是指阻止入侵者试图控制自己的系统或者网络资源的安全保护机制，而漏洞扫描是指基于漏洞数据库，通过扫描手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，不属于入侵检测技术。

答案：D

例 8-29　IDS 设备的主要作用是 (40) 。(2015 年上半年真题 40)

A. 用户认证　　B. 报文认证　　C. 入侵检测　　D. 数据加密

解析：IDS 是入侵检测系统的英文缩写，全称为 Intrusion Detection System，顾名思义，IDS 设备的主要作用是对网络中的入侵行为进行检测。

答案：C

8.13.3 同步练习

在入侵检测系统中，事件分析器接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其常用的三种分析方法不包括________。

A. 模式匹配　　B. 密文分析　　C. 数据完整性分析　　D. 系统分析

8.13.4 同步练习参考答案

B

8.14 入侵防御系统

8.14.1 考点辅导

在网络安全领域，入侵防御系统(Intrusion Prevention System，IPS)是随着网络的高速发展而产生的。IPS 是在入侵检测系统(Intrusion Detection System，IDS)的基础之上发展起来的，它不仅具有入侵检测系统检测攻击行为的能力，而且具有防火墙拦截攻击并且阻断攻击的功能，但是 IPS 并不是 IDS 的功能与防火墙功能的简单组合，IPS 在攻击响应上采取的是主动的、全面的、深层次的防御。

1. 入侵防御系统的概念

随着市场需求的变化和应用领域的不同，入侵防御系统在具体的功能实现方面，不同的系统具有不同的特征，但是其核心功能是检测与防御。目前对入侵防御系统的定义也是多种多样的，一种定义是：入侵防御系统是一种抢先的网络安全检测和防御系统，它能检测出攻击并快速做出回应。还有一种对 IPS 的定义：IPS 是一种能够检测出网络攻击，并且在检测到攻击后能够积极主动响应攻击的软硬件网络系统。

2. 入侵防御系统与入侵检测系统的区别

入侵检测系统有效地弥补了防火墙系统对网络上的入侵行为无法识别和检测的不足，入侵检测系统的部署，使得在网络上的入侵行为得到了较好的检测和识别，并能够进行及时的报警。然而，随着网络技术的不断发展，网络攻击类型和方式也在发生着巨大的变化，入侵检测系统也逐渐地暴露出如漏报、误报率高、灵活性差和入侵响应能力较弱等不足之处。

入侵防御系统是在入侵检测系统的基础上发展起来的，入侵防御系统不仅能够检测到网络中的攻击行为，同时能够主动地对攻击行为发出响应，对攻击进行防御。两者相较，主要存在以下几种区别。

1)　在网络中的部署位置的不同

IPS 一般是作为一种网络设备串接在网络中的，而 IDS 一般是采用旁路挂接的方式，连接在网络中。

2)　入侵响应能力的不同

IDS 设备对于网络中的入侵行为，往往是采用将入侵行为记入日志，并向网络管理员发出警报的方式来处理的，对于入侵行为并不主动采取对应措施，响应方式单一；而入侵防御系统检测到入侵行为后，能够对攻击行为进行主动的防御，例如丢弃攻击连接的数据包以阻断攻击会话，主动发送 ICMP 不可到达数据包、记录日志和动态的生成防御规则等多种方式对攻击行为进行防御。

3. IPS 的优势与局限性

与 IDS 系统相比较，IPS 具有其自身的特点，其优点主要表现在以下几个方面。

(1)　积极主动地防御攻击。

(2)　具有较深的防御层次。

其不足之处主要表现在以下几个方面。

(1)　容易造成单点故障。

(2)　漏报和误报。

(3)　性能瓶颈。

8.14.2　典型例题分析

例 8-30　(65)　不属于入侵检测技术。(2017 年下半年真题 65)

A. 专家系统　　B. 模型检测　　C. 简单匹配　　D. 漏洞扫描

解析：入侵检测技术是指阻止入侵者识图控制自己的系统或者网络资源的安全保护机制，而漏洞扫描是指基于漏洞数据库，通过扫描手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，不属于入侵检测技术。

答案：D

8.14.3　同步练习

为了防止电子邮件中的恶意代码，应该用________方式阅读电子邮件。

A. 纯文本　　B. 网页　　C. 程序　　D. 会话

8.14.4　同步练习参考答案

A

8.15 本章小结

本章知识点在2014年的新大纲中变化不大，只是对一些表述方式做了相应的调整。

本章主要要求考生掌握网络安全基础知识和技术，包括保密、安全体制、安全协议、病毒防范、入侵检测、访问控制与防火墙、数字证书、VPN 配置及PGP的知识。需要考生重点掌握。

本章相关知识点在历次考试中都会有所涉及，分值在 9 分左右，是考试的重点。对网络安全的学习关键要以加密技术为基础，其他所有网络安全技术手段都是建立在密钥加密的基本方法之上的不同应用，所以必须抓住重点。本章前几节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

8.16 达标训练题及参考答案

8.16.1 达标训练题

1. 网络的可用性是指________。

A. 网络通信能力的大小　　B. 用户用于网络维修的时间

C. 网络的可靠性　　D. 用户可利用网络时间的百分比

2. 利用三重DES进行加密，以下说法正确的是________。

A. 三重DES的密钥长度是56位　　B. 三重DES使用3个不同的密钥进行加密

C. 三重DES的安全性高于DES　　D. 三重DES的加密速度比DES快

3. 在Wi-Fi安全协议中，WPA与WEP相比，采用了________。

A. 较短的初始化向量　　B. 更强的加密算法

C. 共享密钥认证方案　　D. 临时密钥以减少安全风险

4. SDES是一种________算法。

A. 共享密钥　　B. 公开密钥

C. 报文摘要　　D. 访问控制

5. 公钥体系中，用户甲发送给用户乙的数据要用________进行加密。

A. 甲的公钥　　B. 甲的私钥

C. 乙的公钥　　D. 乙的私钥

6. 用户B收到用户A带数字签名的消息M，为了验证M的真实性，首先需要从CA获取用户的数字证书，并利用__(1)__验证该证书的真伪，然后利用__(2)__验证 *M* 的真实性。

(1)、(2) A. CA的公钥　　B. B的私钥

C. A的公钥　　D. B的公钥

7. 甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息后利用________验证该消息的真实性。

A. 甲的公钥　　B. 甲的私钥　　C. 乙的公钥　　D. 乙的私钥

8. 利用报文摘要算法生成报文摘要的目的是________。
   A. 验证通信对方的身份，防止假冒
   B. 对传输数据进行加密，防止数据被窃听
   C. 防止发送方否认发送过的数据
   D. 防止发送的报文被篡改

9. 使用路由器对局域网进行分段的好处是________。
   A. 广播帧不会通过路由器进行转发
   B. 通过路由器转发减少了通信延迟
   C. 路由器的价格便宜，比使用交换机更经济
   D. 可以开发新的应用

10. 下列安全协议中，与 TLS 功能相似的协议是________。
    A. PGP　　B. SSL　　C. HTTPs　　D. IPSec

11. IPSec 中安全关联(Security Associations)三元组是________。
    A. <安全参数索引(SPI)，目标 IP 地址，安全协议>
    B. <安全参数索引(SPI)，源 IP 地址，数字证书>
    C. <安全参数索引(SPI)，目标 IP 地址，数字证书>
    D. <安全参数索引(SPI)，源 IP 地址，安全协议>

12. ________是支持电子邮件加密的协议。
    A. PGP　　B. PKI　　C. SET　　D. Kerberos

13. 下面能正确表示 L2TP 数据包的封装格式的是________。

A.

IP	TCP	L2TP	PPP

B.

IP	UDP	L2TP	PPP

C.

IP	L2TP	TCP	PPP

D.

IP	L2TP	UDP	PPP

14. 支持安全 Web 服务的协议是________。
    A. HTTPs　　B. WINS　　C. SOAP　　D. HTTP

15. 安全电子邮件使用________协议。
    A. PGP　　B. HTTPs　　C. MIME　　D. DES

16. 如果一台 CISIO PLX 防火墙有如下的配置：

```
PLX(config)#nameif etherent0 f1 security0
PLX(config)#nameif etherent1 f2 security00
PLX(config)#nameif etherent2 f3 security50
```

那么以下说法，正确的是________。
   A. 端口 f1 作为外部网络接口，f2 连接 DMZ 区域，f3 作为内部网络接口
   B. 端口 f1 作为内部网络接口，f2 连接 DMZ 区域，f3 作为外部网络接口
   C. 端口 f1 作为外部网络接口，f2 作为内部网络接口，f3 连接 DMZ 区域

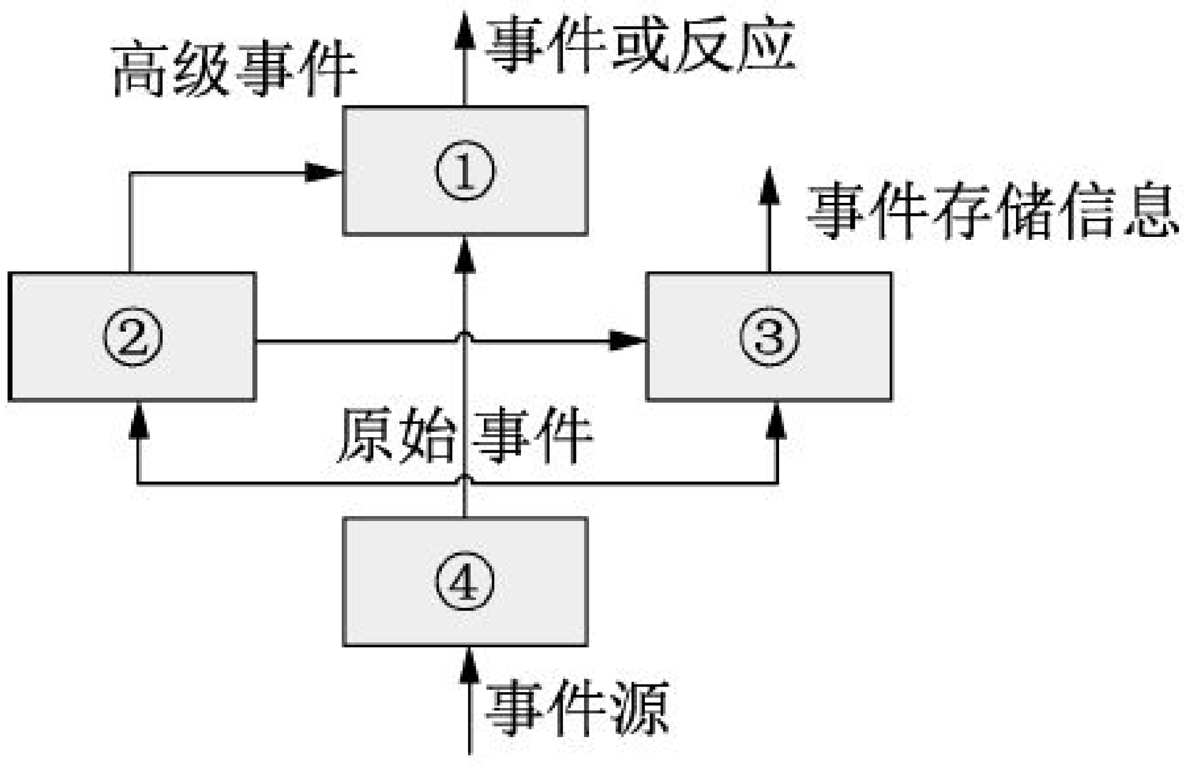
D. 端口 f1 作为内部网络接口，f2 作为外部网络接口，f3 连接 DMZ 区域

17. 近年来，在我国出现的各类病毒中，________病毒通过木马形式感染智能手机。

A. 欢乐时光　　B. 熊猫烧香

C. X 卧底　　D. CIH

18. 下图为 DARPA 提供的公共入侵检测框架示意图，该系统由 4 个模块组成，其中模块①～④对应的正确名称为________。



A. 事件产生器、事件数据库、事件分析器、响应单元

B. 事件分析器、事件产生器、响应单元、事件数据库

C. 事件数据库、响应单元、事件产生器、事件分析器

D. 响应单元、事件分析器、事件数据库、事件产生器

19. 以下关于钓鱼网站的说法中，错误的是________。

A. 钓鱼网站仿冒真实网站的 URL 地址

B. 钓鱼网站是一种网络游戏

C. 钓鱼网站用于窃取访问者的机密信息

D. 钓鱼网站可以通过 E-mail 传播网址

8.16.2　参考答案

1. D	2. C	3. D	4. A	5. C
6. (1) A　(2) C	7. A	8. D	9. A	10. B
11. A	12. A	13. B	14. A	15. A
16. C　17. C	18. D	19. B		

第 9 章　网络操作系统与应用服务器配置

大纲要求：

- 网络操作系统的功能、分类和特点。
- Windows Server 2008 R2。
- DHCP 服务器的原理和配置(Windows)。
- 网络系统管理，包括 Windows 系统、Windows 活动目录、Windows 终端服务与远程管理。
- DNS，包括域名解析、DNS 服务器的配置(Windows)。
- 电子邮件服务器配置(Windows)。
- WWW，包括虚拟主机、WWW 服务器配置(Windows)、WWW 服务器的安全配置。
- FTP 服务器，包括 FTP 服务器的访问、FTP 服务器的配置(Windows)。

9.1　网络操作系统

9.1.1　考点辅导

网络操作系统(Network Operating System，NOS)是使网络上各计算机能方便而有效地共享网络资源，为网络用户提供所需的各种服务的软件和有关规程的集合。所述可共享的网络资源包括硬件(传输介质、服务器等)、软件(系统程序、实用程序、应用程序等)及数据。

9.1.1.1　网络操作系统的基本概念

1. 网络操作系统的特征

网络操作系统除具备单机操作系统的四大特征，即并发、资源共享、虚拟和异步性外，还引入了开放性、一致性和透明性。

1)　开放性

为了便于把配置了不同操作系统的计算机系统互联起来形成计算机网络，使不同的系统之间能协调地工作，实现应用的可移植性和互操作性，而且能进一步将各种网络互联起来组成互联网，国际标准化组织(ISO)推出了开放系统互联参考模型(OSI-RM)。各大计算机厂商为此纷纷推出其相应的开放体系结构和技术，并成立多种国际性组织以促进开放性的实现。例如，由 IBM、DEC、HP 等组成了开放软件基金会(OSF)，并为开放系统制定了一套应用环境规范(AES)。

又如，国际性组织 X/OPEN 也依据事实上的标准和相应的国际标准定义了 X/OPEN 的公共应用环境(CAE)。

2) 一致性

由于网络可能是由多种不同的系统所构成的，为了方便用户对网络的使用和维护，要求网络具有一致性。网络的一致性是指网络向用户、低层向高层提供一个一致性的服务接口，该接口规定了命令(服务原语)的类型、命令的内部参数及合法的访问命令序列等，并不涉及服务接口的具体实现。例如，功能的实现是采用过程方式还是进程方式，或者其他方式，可由程序自行确定，正因为如此，在 OSI-RM 中规定了各个层次的服务接口，各种协议也都规定了服务接口，通过对这些接口的定义确保网络的一致性。例如，在不同的系统间交换文件时，尽管各系统的文件子系统可能采用不同的文件结构和存取方法，但只要利用 FTAM 中所提供的一套文件服务原语，就可实现不同系统之间的文件传输。换句话说，FTAM 屏蔽了不同文件系统之间的差异，网络用户可以用一致的方法访问网络中的任何文件。

3) 透明性

一般来说，透明性即指某一实际存在的实体的不可见性，也就是对使用者来说，该实体看起来是不存在的。在网络环境下的透明性，表现得十分明显，而且显得十分重要，几乎网络提供的所有服务无不具有透明性，即用户只需知道他应得到什么样的网络服务，而无须了解该服务的实现细节和所需资源。事实上，由于用户通信和资源共享的实现都是极其复杂的，因此，如果 NOS 不具有透明性这一特征，用户将难以甚至根本不可能去使用网络提供的服务。例如，一个网络工作站用户访问远程资源时就像访问本地资源一样方便，两者采用同样的方法，使用户感觉不到他在访问远程资源时所提出的请求，可能跨越了千山万水，网络为实现该服务而执行了大量的操作(从源主机的应用层逐层下达至物理层后，再经过网络到达目标主机，然后由目标主机的物理层逐层上传到应用层，最后才访问到远地资源。访问结果再以相反的传递过程回馈给用户)。

2. 网络操作系统的安全性

网络操作系统的安全性非常重要，表现在以下几个方面。

(1) 用户账号安全性。使用网络操作系统的每一个用户都有一个系统账号和有效的口令字。在一些早期版本中，口令字是以非加密方式在局域网中传输的，随着协议分析仪的广泛应用，非加密口令字具有明显缺陷，协议分析仪可以检测局域网中的每一个信息包，很容易查看到用户工作站在注册过程中所发送的口令字，为此必须在用户工作站发送口令字之前对口令字进行加密。

(2) 时间限制。系统管理员对每个用户的注册时间进行限定，限定方式以一定的时间间隔为单位，如半小时间隔方式、星期几的方式等。时间限制功能主要应用在要求具有严格安全机制的网络环境中。

(3) 站点限制。系统管理员对每一用户注册的站点进行限定。站点限定了每个用户只能在指定物理地址的工作站上进行注册。这样就阻止了企图从其他区域使用不同于自己的工作站而进行注册，能在一定程度上确保安全性。

(4) 磁盘空间限制。系统管理员对每个用户允许使用的磁盘服务器磁盘空间加以限定，以防止可能出现的某些用户无限制侵占服务器磁盘的情况发生，确保其他用户磁盘空间的安全性。

(5) 传输介质的安全性。由于局域网的传输介质——同轴电缆和双绞线很容易被窃听，

并将数据读走，因此网络传输介质的安全性也是十分重要的。为此在一些机密环境中，可以将网络电缆安装在导管内，防止由于电磁辐射而使数据被窃听。也可将网络电缆线预埋在混凝土内，避免对网络电缆的物理挂接。从安全性考虑，网络传输介质应是光缆，因为对光缆的窃听非常困难。

(6) 加密。对数据库和文件进行加密是保证文件服务器数据安全性的重要手段。一般在关闭文件时加密，在打开文件时解密。加密后具有超级用户特权的网络管理员才能读取服务器上的目录和文件。很多数据库系统都具有对数据文件进行加密的功能。平常所遇到的许多加密程序是与某些软件工具一起提供的。

(7) 审计。网络的审计功能可以帮助网络管理员对那些企图对网络操作系统实行窃听行为的用户进行鉴别。当对网络运行机理熟练的某用户通过多次重复输入口令字来试探其他用户口令字时，很多网络就采取一定措施来制止这种非法行为。

9.1.1.2 Windows Server 操作系统

Windows Server 2008 是 Microsoft 专为强化下一代网络、应用程序和 Web 服务的功能而设计的操作系统，Windows Server R2 是 Windows Server 2008 的升级版本。这个版本继续提升了虚拟化、系统管理弹性以及信息安全等领域的应用，是一款仅支持 64 位的操作系统，可以为大、中或小型企业搭建功能强大的网站和应用程序服务平台。

Windows Server 2008 R2 增强了核心 Windows Server 操作系统的功能，提供了富有价值的新功能，以协助各种规模的企业提高控制能力、可用性和灵活性，适应不断变化的业务需求。新 Web 工具、虚拟化技术、可伸缩性增强和管理工具有助于节省时间、降低成本，并为信息技术(IT)基础结构奠定坚实的基础。

9.1.1.3 Linux 操作系统

Linux 是一个支持多用户、多任务、多进程和实时性较好的功能强大而稳定的操作系统，也是目前运行硬件平台最广泛的操作系统。Linux 最大的特点在于它是 GNU 的一员，遵循公共版权许可证(GPL)及开放源代码的原则，从而使其成为发展最快、拥有用户最多的操作系统之一。

Red Hat Linux 是目前世界上使用最多的 Linux 操作系统家族成员，提供了丰富的软件包，具有强大的网络服务和管理功能。Red Hat Enterprise Linux 7(有时简写为 RHEL 7)是 Red Hat Linux 的一个最新版本，内核为 Kernel3.10，它在原有的基础上又有了很大的改进，集成了应用程序虚拟化技术 Docker，对 systemd 进程管理器的支持，XFS 成为 RHEL 默认的文件系统以及能监控系统 PCP 等新功能特性，使之较 RHEL 6 在功能和性能方面有很大提升。

9.1.2 典型例题分析

例 9-1 在 Windows 操作系统中，远程桌面使用的默认端口是__(35)__。(2017 年上半年真题 35)

A. 80　　B. 3389　　C. 8080　　D. 1024

解析： 80 为 HTTP 端口，用于网页浏览。1024 为 Reserved 端口，它是动态端口的开始。3389 为远程桌面使用的默认端口。8080 为代理端口，WWW 代理开发此端口。

答案： B

例 9-2 下列不是 NOS 与单机操作系统不同的四大特征的是________。

A. 并发　　B. 资源共享　　C. 虚拟　　D. 同步性

解析： NOS 具备不同于单机操作系统的四大特征是并发、资源共享、虚拟和异步性。

答案： D

9.1.3 同步练习

1. 下列不是 NOS 引入的新特性的是________。
   A. 开放性　　B. 一致性　　C. 透明性　　D. 并发性
2. Windows Server 2003 操作系统中，________提供了远程桌面访问。
   A. FTP　　B. E-mail　　C. Terminal Services　　D. HTTP

9.1.4 同步练习参考答案

1. D　2. C

9.2 网络操作系统的基本配置

9.2.1 考点辅导

9.2.1.1 Windows Server 2008 R2 的本地用户与组

为了保障计算机与网络安全，Windows Server 2008 R2 为不同的用户设置不同的权限，同时通过将具有同一权限的用户设置为一个组来简化对用户的管理。每个登录到 NT Server 上的用户必须有一个用户账号，将具有相同性质的用户归结在一起，统一授权，组成用户组。用户组可分成全局组、本地组和特殊组。

Windows Server 2008 R2 本地用户和组的创建比较简单，用户必须拥有管理员权限，才可以创建用户账户。可以用“服务器管理器”或者“计算机管理”中的“本地用户和组”管理单元来创建本地用户账户。下面以“服务器管理器”为例，说明创建用户账户的主要步骤。

(1) 从“开始”菜单中打开“服务器管理器”窗口，展开左侧的“配置”|“本地用户和组”节点，右击“用户”节点，在弹出的快捷菜单中选择“新用户”命令，如图 9-1 所示。

(2) 在“新用户”对话框中，输入用户名、全名、用户描述信息和用户密码，指定用户密码选项，单击“创建”按钮新增用户账户。创建完用户后，单击“关闭”按钮，如图 9-2 所示。

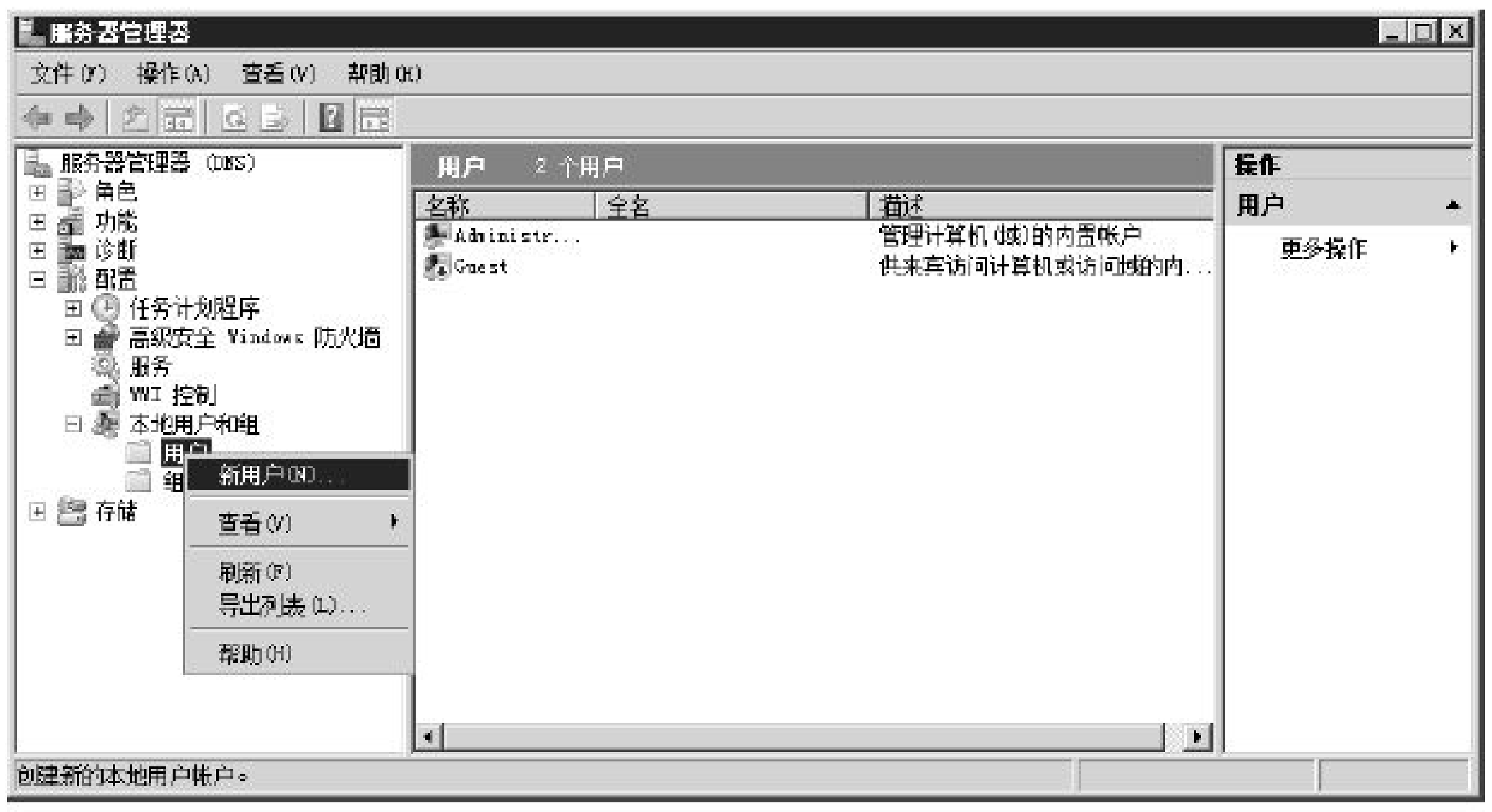


图 9-1　创建用户账户

图 9-2　“新用户”对话框

9.2.1.2　Windows Server 2008 R2 活动目录

1. 活动目录的概念

目录服务是用来存储网络中各种对象(如用户账户、组、计算机、打印机和共享资源等)的有关信息，并按照层次结构方式进行信息的组织，以方便用户的查找和使用，Active Directory(活动目录)是 Windows Server 2008 域环境中提供目录服务的组件。在微软平台上，目录服务从 Windows Server 2000 就开始引入，所以我们可以把 Active Directory 理解为目录服务在微软平台的一种实现方式，当然目录服务在非微软平台上也有相应的实现方式。

活动目录服务是一个完全可扩展、可伸缩的目录服务，系统管理员可在统一的系统环境下管理整个网络中的各种资源，较以往的应用中，Windows Server 2008 有了更加突出的新特性，现介绍如下。

1)　服务的集成性

活动目录的集成性包括内容更丰富，主要体现在 3 个方面：用户及资源的管理、基于目录的网络服务、网络应用管理。Windows Server 2008 活动目录服务采用 Internet 标准协议，用户账户可以使用“用户名@域名”来表示，以进行网络登录。单个域树中所有的域共享一个等级命名结构，与 Internet 的域名空间结构一致。一个子域的名称就是将该名称添加到父域的名称中，例如：hf.xyz.com 就是 xyz.com 域的子域。DNS 是一个 Internet 的标准服务，主要用来将用户的主机名翻译成数字式的 IP 地址。活动目录使用 DNS 为域完成命名和定位服务，域名同时也是 DNS 名。

2)　信息的安全性

Windows Server 2008 系统支持多种网络安全协议，使用这些协议能够获得更强大、更有效的安全性。在活动目录数据库中存储了域安全策略的相关信息，如域用户口令的限制策略和系统访问权限等，由此可实施基于对象的安全模型和访问控制机制。在活动目录中的每个对象都有一个独有的安全性描述，主要是定义了浏览或更新对象属性所需要的访问权限。

3)　管理的简易性

活动目录是以层次结构组织域中的资源。每个域中可有一台或多台域控制器，为了简化管理，用户可在任何域控制器上进行修改，这种更新能复制到所有其他域控制器中的活动目录数据库中。活动目录提供了对网络资源管理的单点登录，管理员可登录环境中任意

一台计算机，来管理网络中的任何计算机的被管理对象。为了使域控制器实现更高的可用性，活动目录允许在线备份。系统管理员通过部署、安装活动目录服务，可以使网络系统环境的管理工作变得更加容易、方便。

4) 应用的灵活性

活动目录具有较强的、自动的可扩展性。系统管理员可以将新的对象添加到应用框架中，并且将新的属性添加到现有对象上。活动目录中可实现一个域或多个域，每个域中有一个或多个域控制器，多个域可合并为域树，多个域树又可合并成为域林。

Windows Server 2008 中的活动目录不仅可以应用到局域网计算机系统环境中，还可以应用于跨地区的广域网系统环境中。

2. *活动目录的物理结构*

活动目录的物理结构分为以下几个部分。

(1) 站点。站点由一个或多个高速连接的 IP 子网构成，这些子网通过高速网络设备连接在一起；站点是网络的物理结构，站点和域没有必然联系，一个站点可包含多个域，一个域也可跨多个站点；创建站点的主要理由是为了优化复制流量和使用户能够用可靠的高速线路连接到域控制器。

(2) 域控制器。域控制器是实际存储活动目录的数据库，用来管理用户登录、验证和目录搜索的任务。

(3) 操作主机。操作主机是活动目录域中负责一个或多个功能的域控制器。

(4) 多主域复制。在 Windows Server 2003 中已采用活动目录的多主域复制方式，即每台域控制器都维护着活动目录的口读/写的副本，管理其变化和更新。在一个域中各域控制器之间相互复制活动目录的改变。在一个目录林中，各域控制器之间把某些信息自动复制给对方。

提示：Windows Server 2003 *采用了多主机的复制模式，多个域控制器没有主次之分。*

在活动目录数据库中允许用户创建各种对象，操作非常简单。只需在“Active Directory 用户和计算机”控制台窗口单击域控制器名，然后在右侧窗口空白处单击鼠标右键，在弹出的快捷菜单中选择“新建”命令，就可以创建用户需要的对象类型了，如图 9-3 所示。

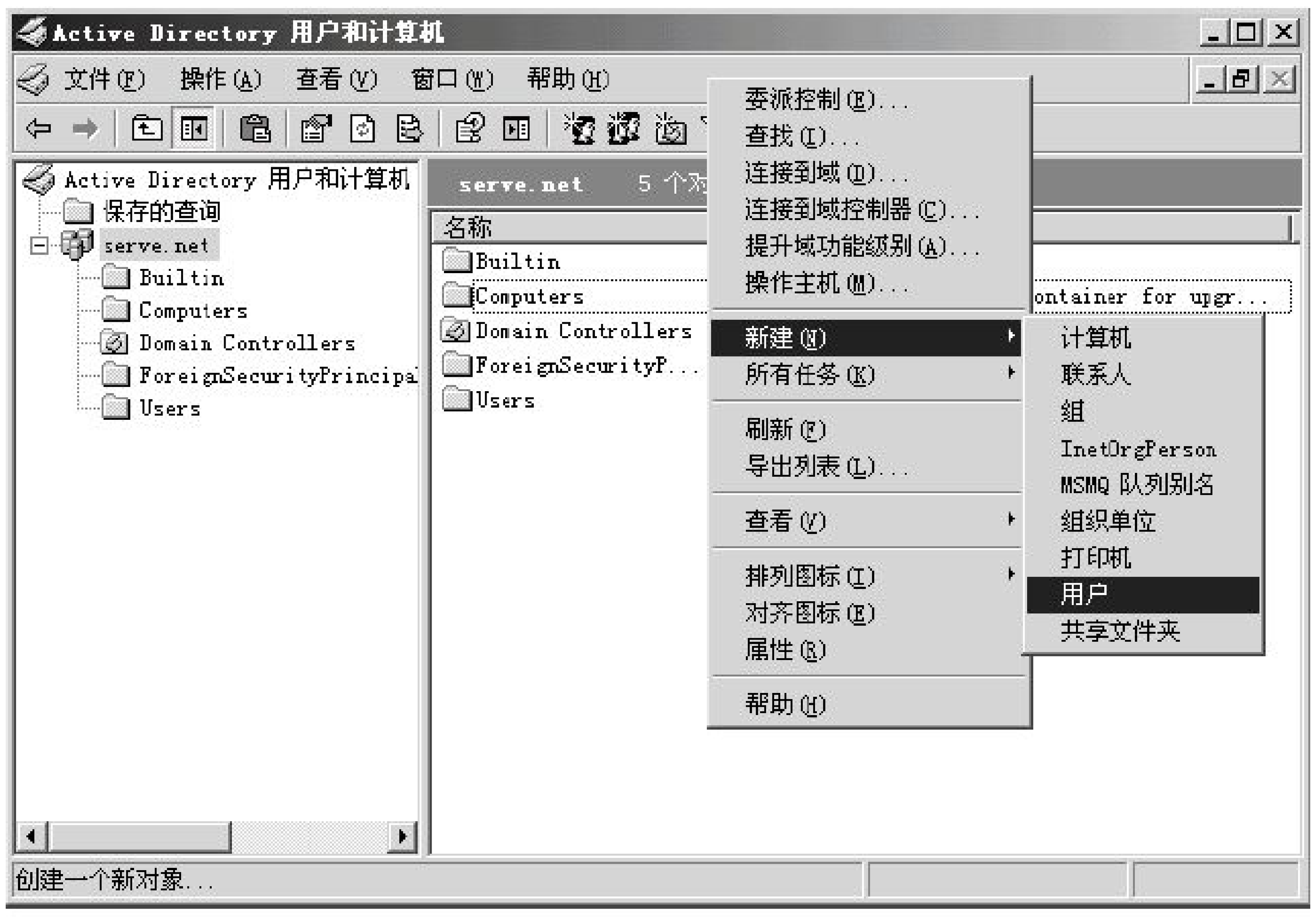


图 9-3 创建活动目录对象

9.2.1.3　Windows Server 2008 R2 远程桌面服务

终端服务提供通过作为终端仿真器工作的“瘦客户”软件远程访问服务器桌面的能力。终端服务基本由 3 个部分组成：客户端部分、协议部分及服务器部分。在客户端安装名为“远程桌面”的程序后，就可以看到服务器完全一致的计算机桌面，并能执行一样的操作。犹如将服务器搬到自己眼前一样。客户端和服务器通过远程桌面协议进行通信。

在 Windows Server 2008 R2 中，终端服务也没有被默认安装，需要手动添加。具体步骤为：依次选择“开始”→“管理工具”→“配置您的服务器向导”命令，在打开的“配置您的服务器向导”对话框中，单击“下一步”按钮；按照“预备步骤”窗口中的说明操作，单击“下一步”按钮；在“服务器角色”对话框，选择“终端服务器”选项，单击“下一步”按钮；按照向导中的说明操作来完成安装。

默认情况下只有系统管理员组用户(Administrators)和系统组用户(SYSTEM)拥有访问和完全控制终端服务器的权限，另外，远程桌面用户组(Remote Desktop Users)的成员只拥有访问权限而不具备完全控制权。而在很多时候，默认的权限设置往往并不能完全满足实际需求，因此还需要赋予某些特殊用户远程连接的权限。具体操作如下。

依次选择“开始”→“管理工具”→“终端服务配置”命令，在打开的“终端服务配置”对话框中，双击右侧窗格中的 RDP-Tcp 连接。打开“RDP-Tcp 属性”对话框，切换到“权限”选项卡，如图 9-4 所示。在“权限”选项卡中可以设置有哪些用户和组可以从客户端登录该终端服务器。

图 9-4　“权限”选项卡

9.2.1.4　Windows Server 2008 R2 远程管理

远程管理的使用与活动目录和组策略的使用一样重要，是衡量 Windows Server 2008 R2 网络管理员、系统管理员水平的重要指标。

在 Windows Server 2008 R2 家族操作系统中，进行远程管理的方法是多种多样的，主要包括 MMC(微软管理控制台)法、远程桌面连接法、管理远程桌面(终端服务)法、管理工具方法、远程协助法、Telnet 法、远程管理 Web 法和远程存储法。

1. 微软管理控制台(MMC)

微软管理控制台集成了用来管理网络、计算机、服务及其他系统组件的管理工具。但 MMC 不执行管理功能，可以使用 MMC 创建、保存并打开管理工具单元，这些管理工具用来管理软件、硬件和 Windows 系统的网络组件。

使用 MMC 有以下两种方法。

① 在用户模式中使用已有的 MMC 控制台管理系统。

② 创建新控制台或修改已有的 MMC 控制台。

2. 远程桌面连接

1) 配置远程桌面连接

要想成功连接到终端服务器，必须保证服务器允许进行“远程桌面”连接。右键单击“我的电脑”，在弹出的快捷菜单中选择“属性”命令，打开“远程”选项卡，选中“允许用户远程连接到您的计算机”复选框。

2) 使用桌面连接

用户要想远程连接到终端服务器，首先需要安装客户端。安装完客户端后执行以下操作就可以连接到终端服务器。

依次选择“开始”→“所有程序”→“附件”→“远程桌面连接”命令，在打开的“远程桌面连接”对话框中，单击“选项”按钮，切换到详细的登录对话框，如图 9-5 所示。输入终端服务器的 IP 地址、用户名、密码，并单击“连接”按钮。出现 Windows 登录对话框后输入已授权的用户名的密码即可完成连接。

图 9-5　运行远程访问服务

9.2.1.5　Linux 网络配置

1. 网络配置文件

系统中重要的网络配置文件有/etc/sysconfig/network、/etc/hostname、/etc/hosts、/etc/services、/etc/host.conf、/etc/nsswitch.conf 及/etc/resolv.conf 等。下面介绍这些文件。

- /etc/sysconfig/network，这个网络文件中包含了控制与网络有关的文件和守护程序的行为的参数。

- /etc/hostname 文件只包含主机的名称。这个文件是在启动时从文件/etc/sysconfig/network 中的 hostname 行中得到的。这个文件用于在启动时设置系统的主机名。
- /etc/hosts 文件中包含 IP 地址和主机名之间的映射，还包括主机名的别名。
- /etc/services 文件中包含端口号和服务器名之间的映射。
- /etc/host.conf 文件声明了命名系统的顺序(/etc/hosts 文件、DNS、NIS)，这些命名系统用来解析主机名。
- /etc/nsswitch.conf 文件是由 Sun 公司开发并用于管理系统中多个配置文件查找顺序的，它比/etc/host.conf 文件提供了更多的功能。
- /etc/resolv.conf 文件配置 DNS 客户。它包含主机的域名搜索顺序和 DNS 服务器的地址。

2. 网络配置命令

1)　配置主机网络接口命令：ifconfig

程序/sbin/ifconfig 用来配置主机网络接口。这包括基本的配置，如 IP 地址、掩码和广播地址，以及高级的选项，如为点对点连接(如 PPP 连接)设置远程地址。

一个接口可以在不进行重新配置的情况下临时地变为不可用和再变为可用。可以用于将服务器的网络连接临时变为不可用(当重新配置一个服务时)。使用下列命令实现本功能。

```
ifconfig interface down    关闭接口
ifconfig interface ip-address up 启动接口
```

如：

```
#ifconfig eth0 192.168.0.2 netmask 257-257-257-0 up
```

2)　处理路由表命令：route

/sbin/route 命令操纵着内核中的路由表。这个表用于了解在数据包离开主机后将会完成什么操作(直接发送到目标主机或到某网关)，以及数据包要发送到的网络接口。

route 命令的一般形式为：

```
route [options] [command [parameters]]
```

route 命令可以在路由表中加入或删除路由。使用以下命令完成这种操作。

```
Route add|del [-net|-host] <target> [gw <gateway>] [netmask <netmask>] [[dev]
<interface>]
```

- add 和 del 命令将分别表明是想要增加还是删除一个路由。
- 可选的选项-net 或-host 选项表明是想使操作在一个网络路由中进行还是对一个主机路由。使用它来减少不明确的内容(如地址 10.0.1.0 可以为 C 类网络中的网络地址，或 A 类或 B 类网络中的一个主机的地址)。
- target 参数可以是目标的主机地址或网络数。可以使用关键字 default 作为目标来设置或删除默认路由。
- 可选的 gateway 参数表明这个路由要使用的网关。这个参数如果省略，route 命令将假设主机或网络是直接连到本机的。

3) 网络测试命令：ping

配置完成路由以后，可以用 ping 命令做一个测试来检查一下配置是否成功。ping 命令用于查看网络上的主机是否在工作，它向被查看主机发送 ICMP ECHO_REQUEST 包，正常情况下应该可以接收到响应。ping 命令的一般格式为：

```
ping  [options] [host-name/ip-address]
```

4) 网络查询命令：netstat

/bin/netstat 命令显示所有 TCP/IP 网络服务的状态。根据需要显示的内容，它提供了一些参数。

- netstat 将列出所有连接的套接字。-a(all)选项将列出所有打开的或监听的套接字，而非只是那些有连接的。
- netstat-e(扩展的)选项列出(除了上述的信息)当前使用套接字的用户。
- netstat-r(路由)列出路由表。它列出的信息和不带参数的 netstat 命令得到的输出一致。
- netstat-i(接口)列出网络接口和每一个接口的统计信息。它显示和 ifconfig 得出的同样的统计信息，但以表的形式出现，以便于分析。

9.2.1.6 Linux 文件和目录管理

1. Linux 文件组织与结构

在 DOS、Windows 体系中，每个磁盘或硬盘分区有独立的根目录，并且用唯一的驱动器标识符表示，如 A:、C:等。而 Linux 的文件系统则不一样，它采用了一种虚拟文件系统技术，使不同的磁盘和分区组合成一个整体。单个磁盘或硬盘分区构成单独的文件系统(可以是 FAT、NTFS 等格式)，有其各自的目录树结构。

完整的目录树可划分为较小的部分，这些较小部分又可以单独存放在自己的磁盘或者分区上。这样相对稳定的部分和经常变化的部分可以单独放在不同的分区中，从而可方便备份和系统管理。目录树的主要部分有 root(/)、/usr、/var、/home 等。图 9-6 是一个典型的 Linux 目录结构。

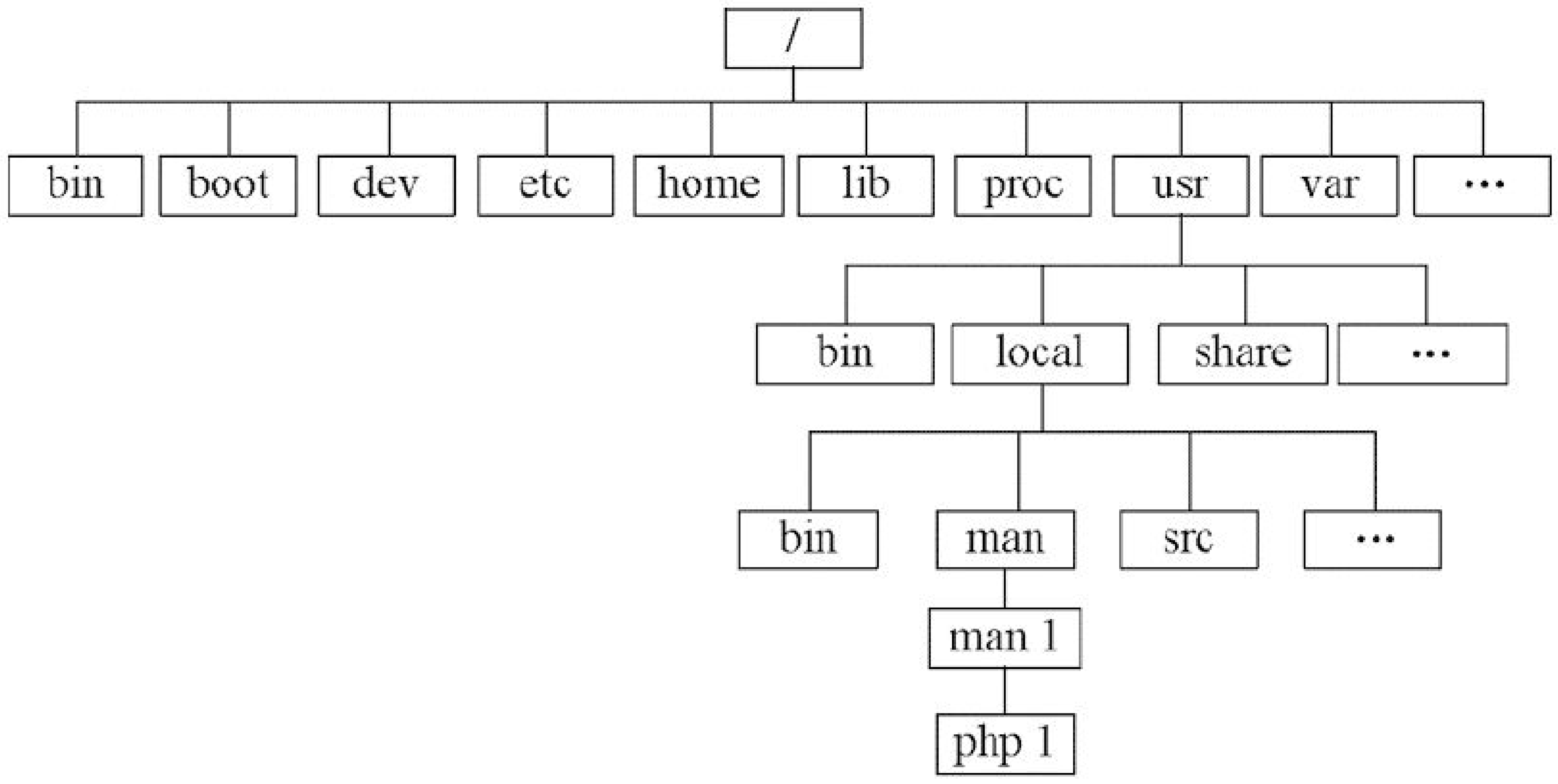


图 9-6 Linux 目录结构

在 Linux 操作系统中有很多目录，要了解下面几个目录的主要内容。

- /bin 目录：该目录存放系统的命令。
- /dev 目录：该目录包含了系统所支持的全部设备的特别文件。
- /etc 目录：该目录包含了系统命令以及一些系统管理配置文件的数据库。
- /lib 目录：该目录包含了 C 语言的标准函数库、数据库以及 C 语言的预处理程序。
- /mnt 目录：这是一个空目录，是专门为接收安装可拆卸的文件系统准备的。
- /tmp 目录：存放临时的文件。
- /usr 目录：用于存放系统中的用户主目录。

2. Linux 文件访问权限

Linux 系统中的每个文件和目录都有访问许可权限，用它来确定用户能以何种方式对文件和目录进行访问和操作。

文件或目录的访问权限分为只读、只写和可执行 3 种。以文件为例，只读权限表示只允许读其内容，而禁止对其做任何的更改操作。可执行权限表示允许将该文件作为一个程序执行。文件被创建时，文件所有者自动拥有对该文件的读、写和可执行权限，以便对文件的阅读和修改。用户也可根据需要把访问权限设置为任何组合。

有 3 种不同类型的用户可对文件或目录进行访问：文件所有者、同组用户、其他用户。文件所有者一般是文件的创建者，他可以允许同组用户访问文件，还可以将文件的访问权限赋予系统中的其他用户，从而使系统中每一位用户都能访问该所有者拥有的文件或目录。

每一文件或目录的访问权限都有 3 组，每组用 3 位表示，分别为文件属主的读、写和执行权限，与属主同组的用户的读、写和执行权限，系统中其他用户的读、写和执行权限。当用 ls -l 命令显示文件或目录的详细信息时，最左边的一列为文件的访问权限。图 9-7 中列出 testvi 这个文件的详细属性，如下：

```
-rw-r--r-- 1 root root 0 10-27 13:05 testvi
```

图 9-7　查看 testvi 文件权限

注意：第一个字符串 r 代表只读，w 代表写，x 代表可执行，这里共有 10 个字符。第一个字符指定了文件类型。在通常意义上，一个目录也是一个文件。如果第一个字符是横线，表示是一个非目录的文件；如果是 d，表示是一个目录。图 9-7 中第二行命令表示 testvi 是一个普通文件，testvi 的属主有读写权限，与 testvi 属主同组的用户只有读权限，其他用户也只有读权限。

3. 文件操作命令

1)　文件复制命令 cp

cp 命令可以将给出的文件或目录复制到另一文件或目录中，如同 DOS 下的 copy 命令一样，功能非常强大。输入下面的命令将 testvi 这个文件复制到/home/tian 目录下：

```
cp testvi /home/tian
```

2) 文件移动命令 mv

mv 命令可以为文件或目录改名或将文件由一个目录移到另一个目录中。mv 命令中第二个参数类型分目标文件和目标目录，如果类型是文件时，mv 命令将所给的源文件或目录重命名为给定的目标文件名，此时，源文件只能有一个(也可以是源目录)；如果是已存在的目录名称时，源文件或目录参数可以有多个，mv 命令将各参数指定的源文件均移至目标目录中。在跨文件系统移动时，mv 先复制，再将原有文件删除，从而连至该文件的链接也将丢失。

3) 文件删除命令 rm

rm 命令提供删除文件功能，该命令可以删除一个目录中的一个或多个文件或目录，它也可以将某个目录及其下的所有文件及子目录均删除。删除单个文件不用带任何参数；如果是删除整个目录及目录下的所有文件，需要带-rf 参数。

4) cat 命令

cat 命令用于在屏幕上滚动显示文件的内容。

5) more 命令

如果文本文件比较长，一屏显示不完，可以使用 more 命令将文件内容分屏显示。每次显示一屏文本，满屏后则停下来，并提示已显示文件内容百分比，按空格键可继续显示下一屏。

6) less 命令

less 命令与 more 命令类似，也是按页显示文件，不同的是 less 命令在显示文件时允许用户既可以向前也可以向后翻阅文件。按 B 键向前翻页显示；按 P 键向后翻页显示；输入百分比显示指定位置；按 Q 键退出显示。

7) mrdir 命令

mrdir 命令的功能是在当前目录中建立一个指定的目录。要求创建目录的用户在当前目录中具有写权限，并且当前目录中没有与之相同的目录或文件名称。

8) 改变目录命令 cd

cd 命令的功能是将当前目录改变到指定的目录，若没有指定目录，则显示用户当前所在的主目录路径。

9) 显示当前目录命令 pwd

pwd 命令的功能是显示用户当前所处的目录，该命令显示整个路径名，并且显示的是当前工作目录的绝对路径。

10) 列目录命令 ls

ls 命令的功能是列出当前目录的内容。对于每个目录，ls 命令将列出其中的所有子目录与文件；对于每个文件，ls 将列出其文件名以及根据命令参数所要求的其他信息。

11) 文件访问权限命令 chmod

chmod 命令用于改变文件或目录的访问权限。只有文件所有者或者超级用户 root 才有权用 chmod 命令改变文件或目录的访问权限。

12) 文件链接命令 ln

ln 命令的功能是在文件之间创建链接。这种操作实际上是给系统中已有的某个文件指定另外一个可用于访问它的名称。

4. Linux 文件类型及操作

Linux 常见的文件类型有普通文件、目录、字符设备文件、块设备文件、套接口文件和符号链接文件等。

1)　普通文件

```
[root@localhost~]# ls -lh install.log
```

用 ls -lh 来查看某个文件的属性，可以看到有类似-rw-r--r--的显示结果，第一个符号是“-”的文件在 Linux 中就是普通文件。这些文件一般是应用程序创建的，如图像工具、文档工具、归档工具或 CP 工具等。这类文件采用 rm 命令进行删除。查看普通文件示例如下：

```
-rw-r--r-- 1 root root 53k 03-16 08:54 install.log
```

2)　目录

目录在 Linux 中是一个比较特殊的文件，其显示结果类似于 drwxr-xr-x，第一个字符是 d。创建目录可以用 mkdir 或 cp 命令，删除目录用 rm 或 rmdir 命令。查看文件及目录的示例如下：

```
[root@localhost ~]# ls -lh
-rw-r--r-- 1 root root    2 03-27 02:00 fonts.scale
-rw-r--r-- 1 root root    53k 03-16 08:54 install.log
-rw-r--r-- 1 root root    14M 03-16 07:53 kernel-2.6.15-1.2025_FC7-i686.rpm
drwxr-xr-x 2 1000 users 4.0k 04-04 23:30 mkuml-2004.09.17
drwxr-xr-x 2 root root  4.0k 04-19 10:53 mydir
drwxr-xr-x 2 root root  4.0k 03-17 04:25 public
```

3)　字符设备或块设备文件

字符设备文件显示结果类似于 crw-rw-rw-，第一个字符是 c，表示 Modem 等串口设备。第一个字符是 b 表示块设备，如硬盘、光驱等设备，使用 mknode 命令来创建的，用 rm 命令来删除。查看字符设备或块设备文件的示例如下：

```
[root@localhost ~]# ls -la /dev/tty
crw-rw-rw- 1 root tty 5, 0 04-19 08:29 /dev/tty
[root@localhost ~]# ls -la /dev/hdal
brw-r----- 1 root disk 3, 1 2006-04-09 /dev/hdal
```

4)　套接口文件

当启动 MySQL 服务器时，会产生一个 mysql.sock 的文件，这个文件属性的第一个字符是 s。查看套接口文件的示例如下：

```
[root@localhost ~]# ls -lh /var/lib/mysql/mysql.sock
srwxrwxrwx 1 mysql mysql 0 04-19 11:12 /var/lib/mysql/mysql.sock
```

5)　符号链接文件

查看符号链接文件的示例如下：

```
[root@localhost ~]# ls -lh setup.log
lrwxrwxrwx 1 root root 11 04-19 11:18 setup.log → install.log
```

第一个字符是 l 的这类文件是链接文件。

9.2.1.7 Linux 用户和组管理

1. 用户管理

在 Linux 操作系统中，每个文件和程序必须属于某一个“用户”，每个用户对应一个账号。在 Linux 操作系统安装后，最重要的用户是超级用户及根用户 root。

超级用户 root 承担了系统管理的一切任务，可以控制所有程序，访问所有文件，使用系统中的所有功能和资源。Linux 系统中其他的一些群和用户都是由 root 来创建的。

用户和组群管理的基本概念如下。

- 用户标记(UID)：系统中用来标识用户的数字。
- 用户主目录：也就是用户的起始工作目录，它是用户在登录系统后所在的目录，用户的文件都放置在此目录下。
- 登录 Shell：用户登录后启动以接收用户的输入并执行输入相应命令的脚本程序。Shell 是用户与 Linux 系统之间的接口。
- 用户组/组群：具有相似属性的多个用户被分配到一个组中。
- 组标识(GID)：用来表示用户组的数字标识。

2. 用户管理命令

一般都使用 Linux 提供的命令 useradd 来添加新用户。创建新用户看似很简单，其实已经在系统里创建了很多东西，该命令默认在/home 下为用户创建了根目录。

出于系统安全考虑，Linux 系统中的每一个用户除了有其用户名外，还有其对应的用户口令。因此使用 useradd 命令创建新用户后，还需使用 passwd 命令为每一位新增加的用户设置口令。root 用户可以使用 passwd 命令改变系统用户的口令，系统用户也可以使用 passwd 命令改变自己的口令。

口令被加密并放入/etc/shdo 文件。选取一个不易被破解的口令是很重要的。应遵守以下规则：口令应该至少有 6 位(最好是 8 位)字符；口令应该是大小写字母、标点符号和数字混杂的。

su 命令提供了用户之间的切换功能，这个命令非常重要，它可以让一个普通用户拥有超级用户或其他用户的权限，也可以让超级用户以普通用户的身份做一些事情。由超级用户切换到普通用户时，无须输入密码；反之，则需要输入超级用户的密码。

3. 用户管理配置文件

与用户和用户组相关的管理信息都存放在一些系统文件中，其中较为重要的文件包括/etc/password、/etc/shadow、/etc/group 等。

(1) /etc/password 文件是 Linux 系统中用于用户管理的最重要的文件。Linux 系统中的每个用户在/etc/password 文件中都有一行对应的记录，每一记录行用冒号分为 7 个域：用户名、加密的口令、用户 ID、组 ID、用户的全名或描述、登录目录、登录 Shell。

(2) /etc/shadow 文件是只有超级用户 root 才能读的文件，该文件包含了系统中所有用户及其口令等相关信息。每个用户在该文件中对应一行，并且用冒号分为 9 个域：用户登录名、用户加密后的口令、从 1970 年 1 月 1 日至口令最近一次被修改的天数、口令在多少

天内不能被用户修改、口令在多少天后必须被修改、口令过期多少天后用户账号被禁止、口令在到期多少天内给用户发出警告、口令自 1970 年 1 月 1 日起被禁止的天数及保留域。

(3)　/etc/group 文件是管理组用户的基本文件，每个组在该文件中有一行记录与之对应，每一行记录用冒号分为 4 个域：用户组名、加密后的组口令、组 ID、组成员列表。

9.2.2　典型例题分析

例 9-3　在 Linux 中，要复制整个目录，应使用__(31)__命令。(2017 年下半年真题 31)

A. cat-a　　B.mv-a　　C. cp-a　　D.rm-a

解析：在 Linux 中 cp 为复制命令。

答案：C

例 9-4　在 Linux 中，__(32)__是默认安装 DHCP 服务器的配置文件。(2017 年下半年真题 32)

A. /etc/dhcpd.conf　　B. /etc/dhcp.conf

C. /var/dhcpd.conf　　D. /var/dhcp.conf

解析：本题考查 Linux 基本配置文件的名字和路径。默认 DHCP 服务器的配置文件是/etc/dhcpd.conf。

答案：A

例 9-5　下面关于 Linux 目录的描述中，正确的是__(31)__。(2017 年上半年真题 31)

A. Linux 只有一个根目录，用“/root”表示

B. Linux 中有多个根目录，用“/”加相应目录名称表示

C. Linux 中只有一个根目录，用“/”表示

D. Linux 中有多个根目录，用相应目录名称表示

解析：在 Linux 中，根目录只有一个，用“/”表示。

答案：C

例 9-6　在 Linux 中，可以使用__(32)__命令为计算机配置 IP 地址。(2017 年上半年真题 32)

A. ifconfig　　B. config　　C. ip-address　　D. Ipconfig

解析：配置主机网络接口命令为 ifconfig。主机网络接口配置包括 IP 地址、掩码和广播地址，以及高级的选项等。

答案：A

例 9-7　在 Linux 中，通常使用__(33)__命令删除一个文件或目录。(2017 年上半年真题 33)

A. rm-I　　B. mv-I　　C. mk-I　　D. cat-i

解析：rm 命令提供删除文件的功能。

答案：A

例 9-8　在 Linux 中，创建权限设置为-rw-rw-r--的普通文件，下面的说法中正确的是__(36)__。(2017 年上半年真题 36)

A. 文件所有者对该文件可读可写

B. 同组用户对该文件只可读

C. 其他用户对该文件可读可写

D. 其他用户对该文件可读可查询

解析：-rw-rw--表示文件所有者可读可写，同组用户可读可写，其他用户只可读。

答案：A

例 9-9 在 Linux 系统中，要查看如下输出，可使用命令__(32)__。(2016 年下半年真题 32)

```
Eth0 Link encap: Ethernet HWaddr 00:20:50:00:78:33
Inet addr:192.168.0.5 Bccast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX:packets:9625272 errors:0 drogped:0 overruns:0 frame:0
TX:packets:6997276 errors:0 drogped:0 overruns:0 frame:0
Collisions:0 txqueuelen:100
Interrupt:19 Base address:0xc800
```

A.[root@localhost]#ifconfig　　B. [root@localhost]#ipconfig eth0

C. [root@localhost]#ipconfig　　D. [root@localhost]#ifconfig eth0

解析：如题输出显示的是网络设备的状态，而 ifconfig 就是 Linux 中用来配置主机网络接口的命令。

答案：A

例 9-10 在 Linux 中，__(41)__命令可将文件以修改时间顺序显示。(2016 年下半年真题 41)

A. Ls-a　　B. Ls-b　　C. Ls-c　　D. Ls-d

解析：在 Linux 中，想要文件以修改时间的顺序显示，可以使用 Ls-c 命令。Is-c 输出文件的 ctime(文件状态最后更改的时间)，并根据 ctime 排序。

答案：C

9.2.3 同步练习

1. 下列关于 Linux 文件组织方式的说法中，________是错误的。
   A. Linux 文件系统使用索引节点来记录文件信息
   B. 文件索引节点号由管理员手工分配
   C. 每个文件与唯一的索引节点号对应
   D. 一个索引节点号可对应多个文件
2. 默认情况下，远程桌面用户组(Remote Desktop Users)成员对终端服务器________。
   A. 具有完全控制权　　B. 具有用户访问权和来宾访问权
   C. 仅具有来宾访问权　　D. 仅具有用户访问权
3. 在 Linux 系统中可用 ls -al 命令列出文件列表，________列出的是一个符号连接文件。
   A. drwxr-xr-x 2 root root 220 2009-04-14 17:30 doe
   B. -rw-r--r-- 1 root root 1050 2009-04-14 17:30 doc1

C. lrwxrwxrwx 1 root root 4096 2009-04-14 17:30 profile

D. drwxrwxrwx 4 root root 4096 2009-04-14 17:30 protocols

4. 在 Linux 系统中，下列关于文件管理命令 cp 与 mv 说法正确的是________。

A. 没有区别　　B. mv 操作不增加文件个数

C. cp 操作不增加文件个数　　D. mv 操作不删除原有文件

5. 在 Linux 系统中，采用__(1)__命令查看进程输出的信息，得到下图所示的结果。系统启动时最先运行的进程是__(2)__，下列关于进程 xinetd 的说法中正确的是__(3)__。

UID	PID	PPID	C	STIME	TTY	TIME	CMD
root	1	0	0	10:10	?	00:00:04	init
root	2	1	0	10:10	?	00:00:00	[keventd]
root	3	1	0	10:10	?	00:00:00	[kapmd]
root	4	1	0	10:10	?	00:00:00	[ksoftirqd-CPU0]
root	9	1	0	10:10	?	00:00:00	[bdflush]
root	5	1	0	10:10	?	00:00:00	[kswapd]
root	6	1	0	10:10	?	00:00:00	[kscand/DMA]
root	1720	1	0	10:11	?	00:00:00	xinetd –stayalive -reuse
root	2074	2072	0	10:48	pts/0	00:00:00	bash
root	2123	2074	0	11:03	pts/0	00:00:00	ps -aef

(1) A. ps -all　　B. ps -aef　　C. ls -a　　D. ls –la

(2) A. 0　　B. null　　C. init　　D. bash

(3) A. xinetd 是网络服务的守护进程　　B. xinetd 是定时服务的守护进程

C. xinetd 进程负责配置网络接口　　D. xinetd 进程负责启动网卡

6. 在 Linux 操作系统中，存放用户账号加密口令的文件是________。

A. /etc/sam　　B. /etc/shadow　　C. etc/group　　D. etc/security

7. 下列关于微软管理控制台(MMC)的说法中，错误的是________。

A. MMC 集成了用来管理网络、计算机、服务及其他系统组件的管理工具

B. MMC 创建、保存并打开管理工具单元

C. MMC 可以运行在 Windows XP 和 Windows 2000 Server 操作系统上

D. MMC 是用来管理硬件、软件和 Windows 系统的网络组件

8. 下列关于 Windows Server 2003 中域的描述，正确的是________。

A. 在网络环境中所有的计算机称为一个域

B. 同一个域中可以有多个备份域控制器

C. 每个域中必须有主域控制器和备份控制器

D. 一个域中可以有多个主域控制器

9. Linux 有 3 个查看文件的命令，若希望能够用光标上下移动来查看文件内容，应使用______命令。

A. cat　　B. more　　C. less　　D. menu

10. Windows 系统下，通过运行______命令可以打开 Windows 管理控制台。

A. regedit　　B. cmd　　C. mmc　　D. mfc

11. 在 Linux 操作系统中，存放有主机名及对应 IP 地址的文件是______。

A. /etc/hostnamc　　B. /etc/hosts

C./etc/resolv.conf　　D. /etc/networks

12. 以下是在 Linux 操作系统中输入 ps 命令后得到的进程状态信息，其中处于“僵死”状态进程的 PID 为__(1)__，若要终止处于“运行”状态的进程的父进程，可以输入命令__(2)__。

```
[root@s1 ~]# ps -el|more
F S UID   PID   PPID C PRI NI ADDR SZ   WCHAN TTY   TIME     COMMAND
4 W  0   9822  9521 0  81 0   -   1220 wait4 pts/2  00:00:00 su
4 S  0   9970  9822 0  75 0   -   1294 wait4 pts/2  00:00:00 bash
1 R  0   15354 9970 0  80 0   -   788    -   pts/2  00:00:00 ps
5 Z  0   17658 9976 0  86 0   -   670    -   pts/2  00:00:03 aio/0
```

(1) A. 9822　　B. 9970　　C. 15354　　D. 17658

(2) A. kill 9822　　B. kill 9970　　C. python 9521　　D. python 9976

9.2.4 同步练习参考答案

1. B　2. B　3. C　4. B　5. (1) B　(2) C　(3) A　6. B
7. D　8. B　9. C　10. C　11. B　12. (1) D　(2) B

9.3 Windows Server 2008 R2 IIS 服务的配置

9.3.1 考点辅导

9.3.1.1 IIS 服务器的基本概念

在组建局域网时，可以利用因特网信息服务器(Internet Information Server，IIS)来构建 WWW 服务器、FTP 服务器和 SMTP 服务器等。IIS 服务提供了一个功能全面的软件包，面向不同的应用领域给出了 Internet/Intranet 服务器解决方案。在 Windows Server 2008 R2 中集成了 IIS 7.5，在 IIS 7.5 模块化的基础上，改进了管理性和功能性，开始支持 ASP.NET、更多的 PowerShell 命令行和集成 WebDAV 等。

1. WWW 服务

WWW(World Wide Web)是图形最为丰富的 Internet 服务。Web 具有很强的链接能力，支持协作和工作流程，可以给分布在世界各地的用户提供商业应用程序。Web 是 Internet 上主机的集合，使用 HTTP 协议提供报文传输服务。基于 Web 的信息使用超文本标记语言，以 HTML 格式传送，它不但可以传送文本信息，还可以传送图形、图像、动画、声音和视频信息。这些特点使得 WWW 成为遍布世界的信息交流平台。

2. FTP 服务

文件传输协议(File Transfer Protocol，FTP)是在 Internet 中两个远程计算机之间传送文件的协议。该协议允许用户使用 FTP 命令对远程计算机中的文件系统进行操作。通过 FTP 可以传送任意类型、任意大小的文件。Windows Server 2008 R2 中 IIS 7.5 里内置了 FTP 模块。

3. SMTP 服务

简单邮件传输协议(Simple Mail Transfer Protocol，SMTP)在客户机应用程序和远程计算机的邮件服务器之间传送邮件信息。也可以通过配置域控制器，使之利用 SMTP 服务跨越站点上的链接实现邮件复制功能。

4. POP3 服务

邮局协议(Post Office Protocol，POP)第 3 版是目前使用最广泛的邮件服务。POP3 的功能是邮件的存储和管理，能为用户提供账号、密码和身份验证功能，与 SMTP 服务配合，提供完整的邮件服务。

9.3.1.2　安装 IIS 服务

IIS 中集成了多种服务，除了可提供 Web 服务外，还提供用于文件传输的 FTP(文件传输协议)服务、用于邮件服务的 SMTP(简单邮件传输协议)服务和用于新闻组的 NNTP(网络新闻传输协议)服务。Windows Server 2008 R2 中集成了最新的 IIS 7.5，IIS 7.5 包含 Web 服务器和 FTP 服务器。

下面介绍 IIS 7.5 的安装方法。

(1) 选择“开始”→“管理工具”→“服务器管理器”命令。打开“服务器管理器”窗口后，选择左侧的“角色”节点，在右窗格的“角色摘要”部分中单击“添加角色”超链接，启动添加角色向导。

(2) 在“开始之前”向导页中提示此向导可以完成的工作，以及操作之前应注意的相关事项，然后单击“下一步”按钮。

(3) 在“选择服务器角色”向导页中显示所有可以安装的服务器角色，如果角色前面的复选框没有选中，表示该网络服务尚未安装，如果已选中，说明该服务已经安装。 这里选中“Web 服务器(IIS)”复选框，如图 9-8 所示。

(4) 系统提示在安装 Web 服务器(IIS)角色时，必须要安装 Windows 进程激活服务功能，否则无法安装 Web 服务器(IIS)角色，单击“添加必需的功能”按钮，如图 9-9 所示。

图 9-8　选择服务器角色

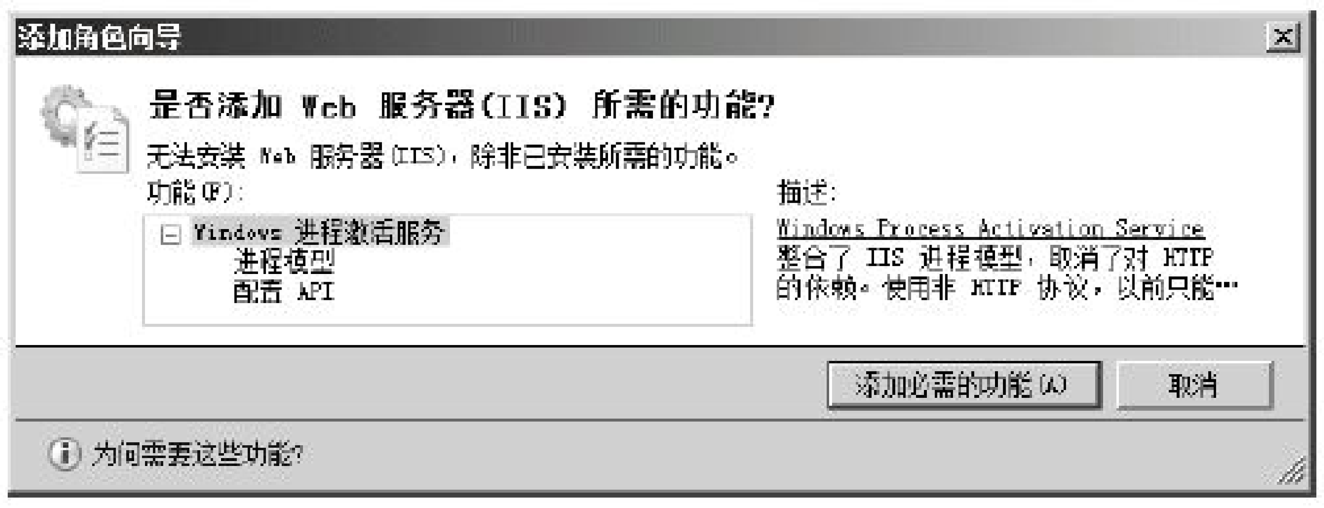


图 9-9　系统提示

(5) 返回“选择服务器角色”向导页后，“Web 服务器(IIS)”复选框被选中，单击“下一步”按钮。

(6) 在“Web 服务器(IIS)简介”向导页中显示了 Web 服务器的功能、注意事项和其他信息，单击“下一步”按钮。

(7) 在“选择角色服务”向导页中默认只选择安装 Web 服务所必需的组件，用户可根据实际需要选择安装的组件。例如，Web 服务器需要使用 ASP.NET 或 ASP，则需要选中相应的复选框。选择完毕后，单击“下一步”按钮，如图 9-10 所示。

(8) 在“确认安装选择”向导页中显示前面所进行的设置，如果选择错误，用户可以单击“上一步”按钮返回。确认无误后，用户可以单击“安装”按钮开始安装 Web 服务器角色，如图 9-11 所示。

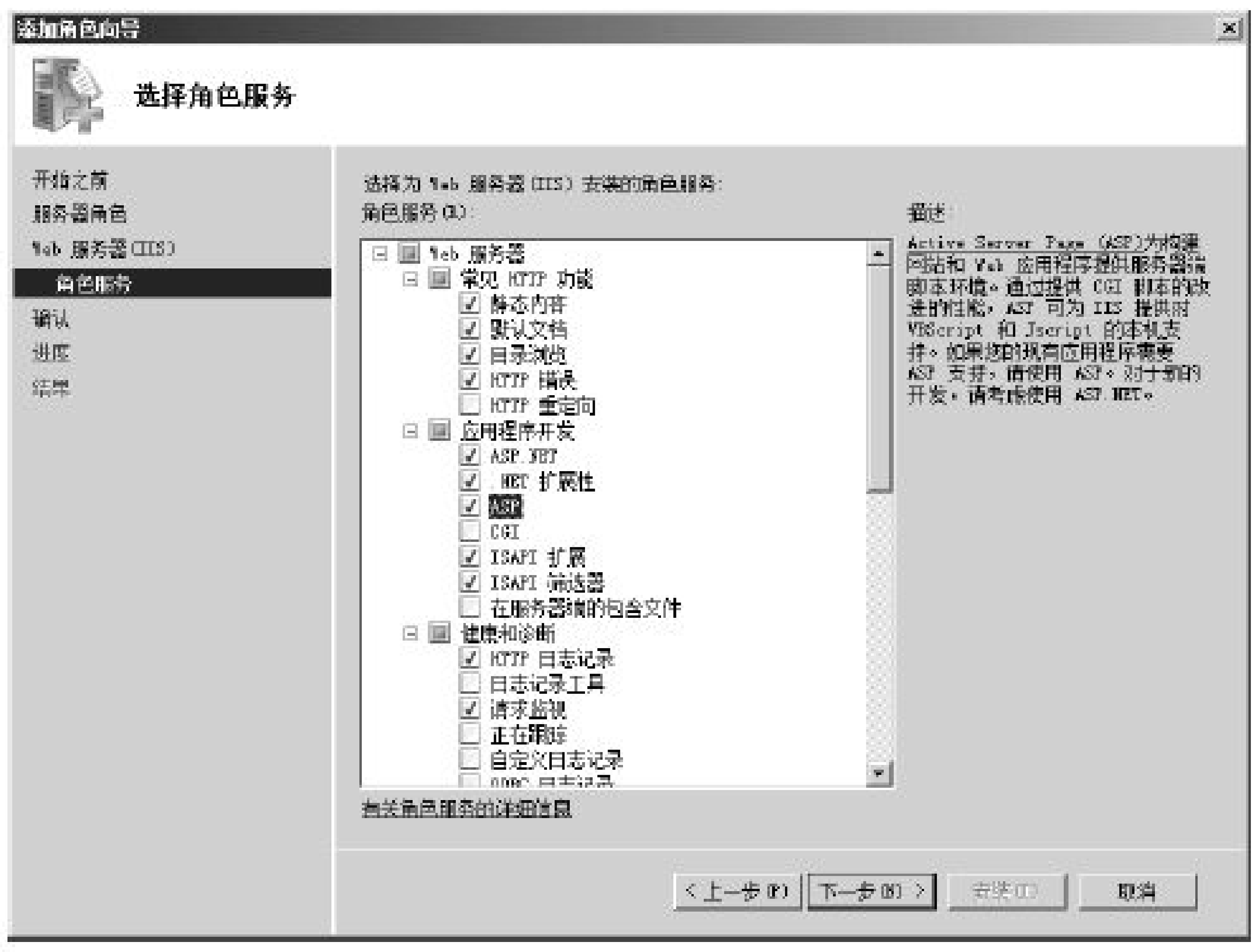


图 9-10 选择角色服务

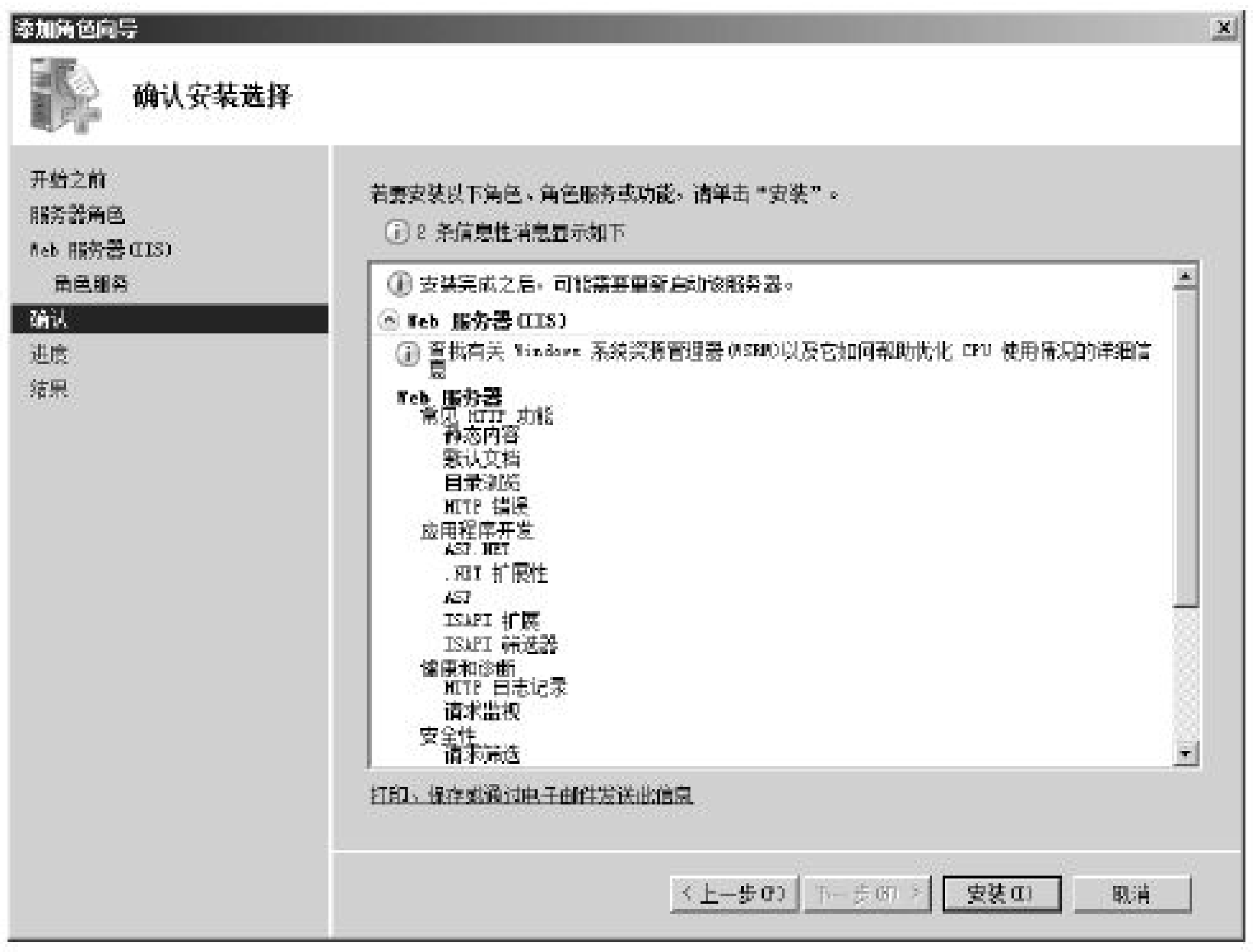


图 9-11 确认安装选择

(9) 在“安装进度”向导页中显示服务器角色的安装过程。

(10) 在“安装结果”向导页中显示安装 Web 服务器(IIS)角色的已经安装，并列出已安装的角色服务。单击“完成”按钮，关闭“添加角色向导”向导页，即可完成 Web 服务器(IIS)角色的安装。

(11) 基于 IIS 的 Web 服务器安装成功后，用户可以通过“Internet 信息服务(IIS)管理器”窗口来管理 Web 站点。打开“Internet 信息服务(IIS)管理器”窗口的方法是选择“开始”→“管理工具”→“Internet 服务管理器”命令。图 9-12 所示的是“Internet 信息服务(IIS)管理器”窗口，从图中可以看出，在安装 IIS 时已创建一个名为 Default Web Site 的 Web 网站。

图 9-12 “Internet 信息服务(IIS)管理器”窗口

(12) 在局域网中的另一台计算机上打开浏览器，在地址栏中输入“http://<服务器 IP 或域名>/”，若能看到如图 9-13 所示的界面，则说明 Web 服务器安装成功。

图 9-13　访问 Default Web Site

9.3.1.3　配置 Web 服务器

IIS 7.5 的 Web 服务组件安装成功后，就可以在这台服务器上创建 Web 站点了。默认情况下，在安装的过程中，系统会自动创建一个默认的 Web 站点。用户可以通过修改默认站点的属性发布自己的 Web 网站，也可以重新建立一个 Web 站点。

1. 网站的基本配置

选择“开始”→“管理工具”→“Internet 服务管理器”命令，打开“Internet 信息服务(IIS)管理器”对话框。在管理器的左侧窗格中单击“网站”节点前的“+”号，然后选中某个希望配置的网站，右键单击该网站，在弹出的快捷菜单中选择“属性”命令，打开网站属性对话框。

在“网站”选项卡中可以设置网站的标识，包括网站描述、IP 地址和端口号，还可以设置连接超时、启用日志记录等，从网站日志记录中可以查看哪些用户访问了网站中的哪些内容，如图 9-14 所示。

在 “主目录”选项卡中指定网站 Web 内容的来源，如图 9-15 所示。

图 9-14　“网站”选项卡

图 9-15　“主目录”选项卡

2. 网站的安全性配置

为了保证 Web 网站和服务器的安全，可以在“目录安全性”选项卡中为网站进行身份验证和访问控制、IP 地址和域名限制的设置，如图 9-16 所示。在“身份验证和访问控制”选项组中单击“编辑”按钮，打开如图 9-17 所示的“身份验证方法”对话框。使用该对话框可以配置 Web 服务器以验证用户身份。可以验证单个用户或选择用户组来阻止未授权用户与受限制内容建立 Web(HTTP)连接。

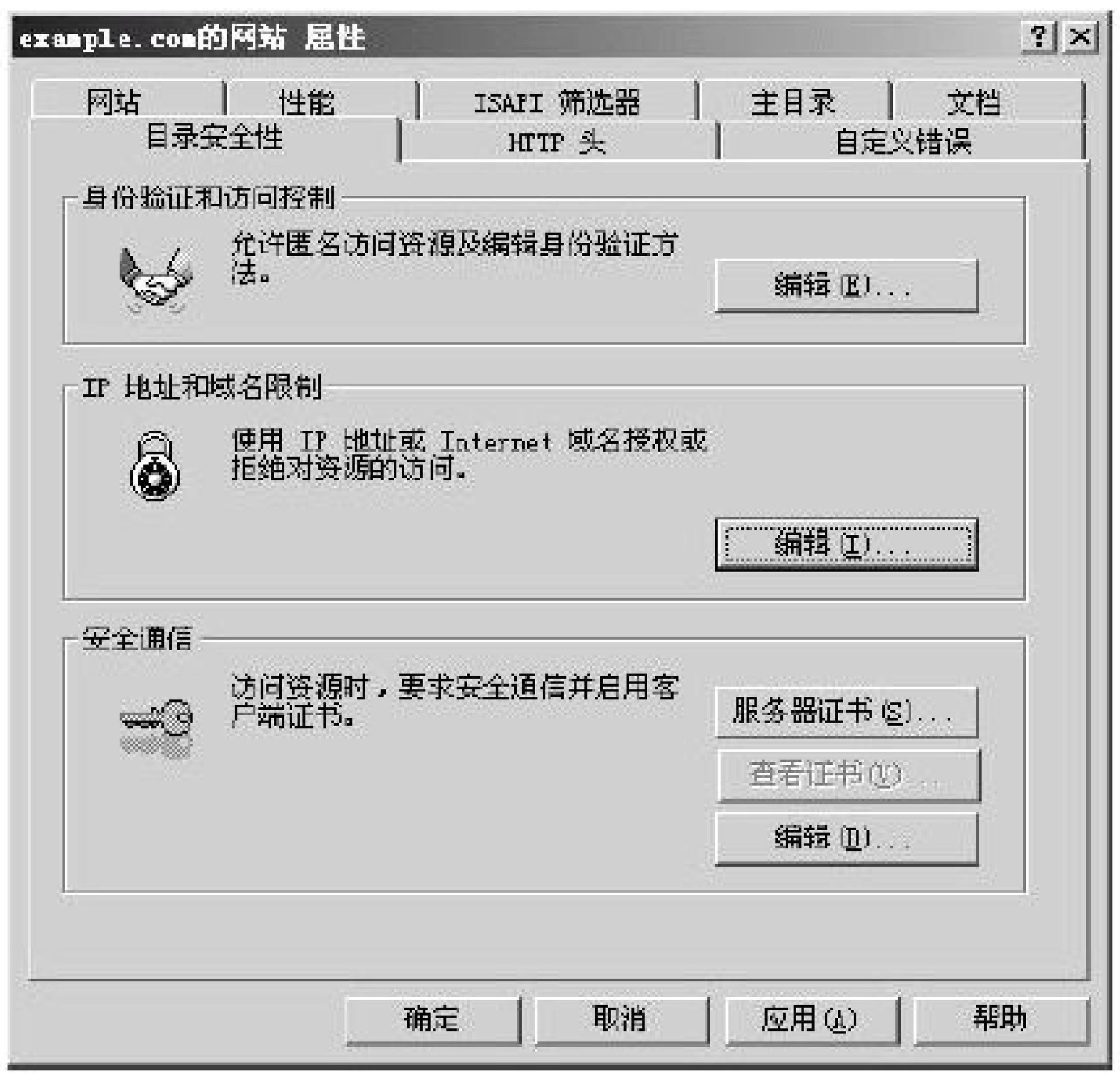


图 9-16 “目录安全性”选项卡

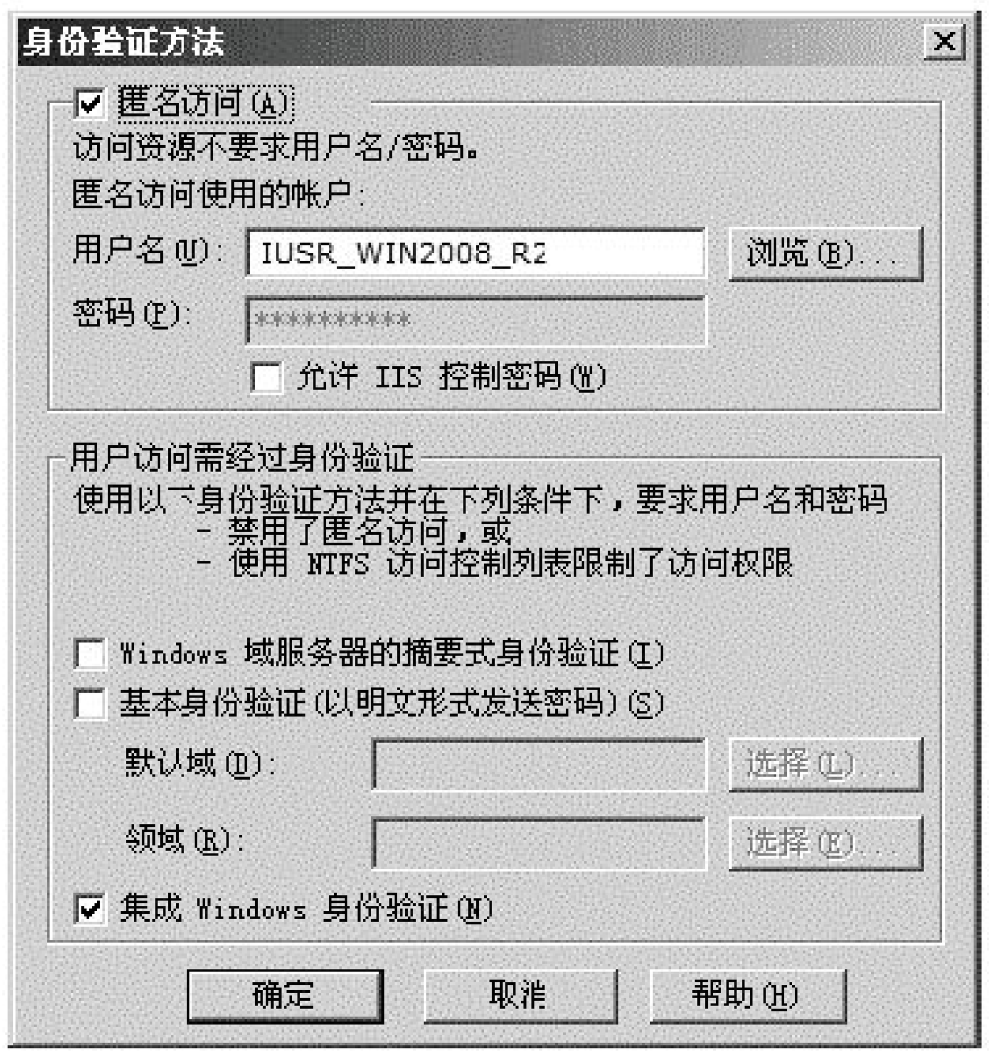


图 9-17 “身份验证方法”对话框

选中“启用匿名访问”复选框可以为用户建立匿名连接，此时用户无须专用的账户，而是使用匿名或来宾账户(Guest)登录到 IIS。默认情况下，服务器创建和使用账户“IUSR_计算机名”，对应于本书所举的例子，用户名为 IUSR_WIN2008_R2。

如果用户希望对网站的访问者验证身份，也可以在“身份验证方法”对话框中的“用户访问需经过身份验证”选项组中进行设置。在此部分中选中的选项要求用户在访问服务器上的任何信息前，提供有效的 Microsoft Windows 用户名和密码。当前 IIS 7.5 中提供了以下两种身份验证方法。

① 基本身份验证。用户使用基本身份验证访问 Web 站点时，系统会模仿为一个本地用户(即能实际登录到 Web 服务器的用户)登录到 Web 服务器，因此用于基本验证的 Windows 用户必须具有“本地登录”用户权限。它是一种工业标准的验证方法，大多数浏览器支持这种验证方法。在使用基本身份验证方法时，用户密码是以未加密形式在网络上传输的，很容易被蓄意破坏系统安全的人在身份验证过程中使用协议分析程序破译用户和密码，因此这种验证方式是不安全的。

② 摘要式身份验证。摘要式身份验证也要求用户输入账号名称和密码，但账号名称和密码都经过 MD5 算法处理，然后将处理后产生的散列随机数(hash)传送给 Web 服务器。采用这种方法时，Web 服务器必须是 Windows 域的成员服务器。

③ 集成 Windows 身份验证。集成 Windows 身份验证是一种安全的验证形式，它也需要用户输入用户账户和密码，但账户名和密码在通过网络发送前会经过散列处理，因此可以确保其安全性。Windows 身份验证方法有两种，分别是 Kerberos v5 验证和 NTLM，如果在 Windows 域控制器上安装了 Active Directory 服务，并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证，否则使用 NTLM 验证。

集成 Windows 身份验证优先于基本身份验证，但它并不先提示用户输入用户名和密码，只有 Windows 身份验证失败后，浏览器才提示用户输入用户名和密码。虽然 Windows 身份验证非常安全，但是在通过 HTTP 代理连接时，Windows 身份验证不起作用，无法在代理服务器或其他防火墙应用程序后使用。因此，Windows 身份验证最适合企业 Intranet 环境。

用户可以基于 IP 地址或域名来允许或拒绝特定用户、计算机、计算机组或域访问该网站、目录或文件。在图 9-16 所示的“IP 地址和域名限制”选项组中单击“编辑”按钮，打开如图 9-18 所示的“IP 地址和域名限制”对话框。默认情况下，所有的计算机都被允许访问该网站。选中“授权访问”单选按钮，可以授权所有的计算机访问该网站，但在“下列除外”列表框中指定的计算机除外。要添加拒绝访问的计算机、计算机组或域，需单击“添加”按钮，打开如图 9-19 所示的“拒绝访问”对话框，在其中输入希望拒绝计算机的相应信息。输入后，单击“确定”按钮，被拒绝访问的计算机将出现在如图 9-18 所示的“下列除外”列表框中。

图 9-18　“IP 地址和域名限制”对话框

图 9-19　“拒绝访问”对话框

9.3.1.4　配置 FTP 服务器

Windows Server 2008 R2 中的 IIS 里内置 FTP 服务模块，安装比较简单。在 FTP 服务安装过程中，安装程序会自动创建一个“默认 FTP 站点”，可以直接修改该站点的属性来满足应用需求。为了更好地管理 FTP 服务器，需要对它进行适当的配置。

在 Internet 信息服务控制台下，右击“默认 FTP”选项，在弹出的快捷菜单中选择“属性”命令，弹出“默认 FTP 站点属性”对话框，如图 9-20 所示。对于“FTP 站点”“安全账户”“主目录”和“目录安全性”的设置基本上与 Web 站点相似，这里就不再赘述了。下面着重介绍“消息”选项卡中的相关设置，打开“消息”选项卡，如图 9-21 所示。

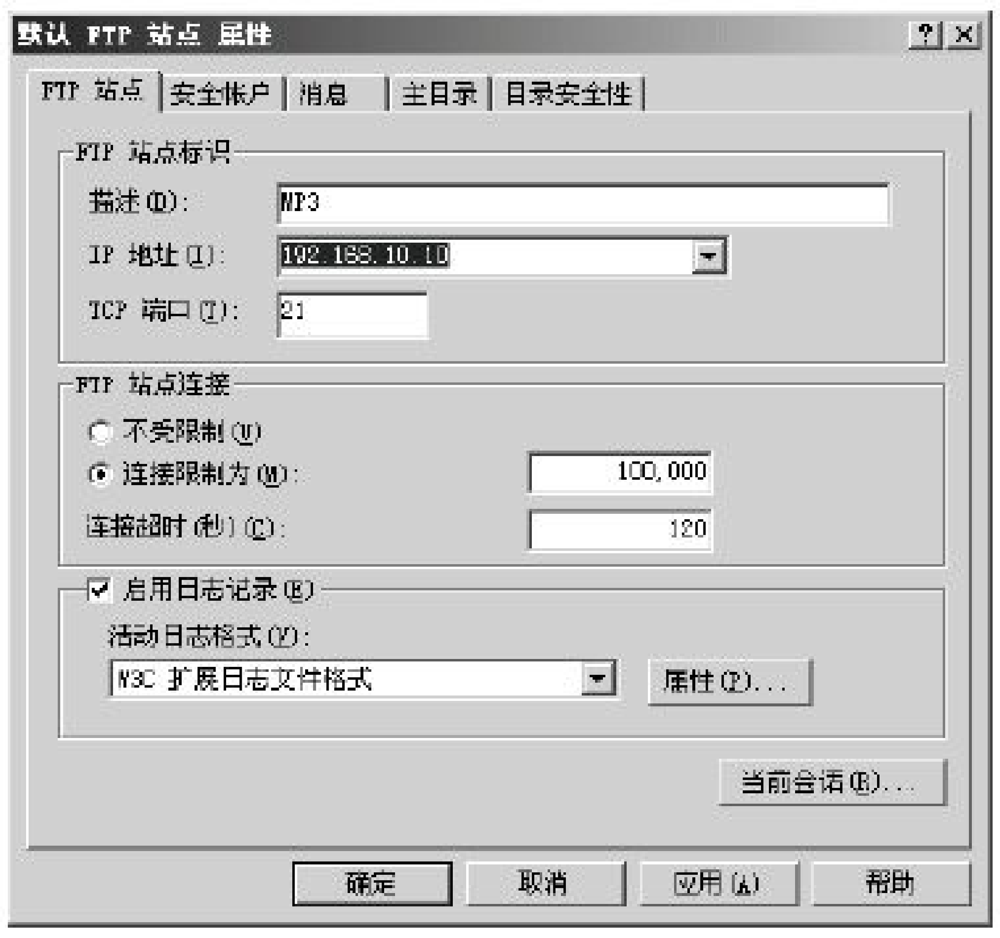


图 9-20　FTP 站点属性

图 9-21　“消息”选项卡

FTP 站点消息的相关设置如表 9-1 所示。

表 9-1 FTP 消息设置

配 置 项	说 明
标题	FTP 的站点名称，用户在登录 FTP 时显示的信息
欢迎	用户登录 FTP 时显示的信息
退出	当用户退出 FTP 时显示的信息
最大连接数	当 FTP 服务器超过最大连接人数时，给提出连接请求的客户机发送一条错误信息

由于服务器配置、性能等的差别，有些服务器不能满足大访问量的需要，往往造成超时甚至死机，因此需要设置连接限制。在图 9-20 所示对话框的“FTP 站点连接”选项组中，有 3 个选项可供选择。

- 不受限制：选中该选项时，将允许同时发生的连接数不受任何限制。
- 连接限制为：选中该选项时，将限制允许同时发生的连接数为某一特定值，这一特定值由用户在文本框中输入。
- 连接超时：选中该选项时，当某条 FTP 连接在一段时间内没有反应时，服务器就自动断开该连接。

9.3.2 典型例题分析

例 9-11 在 Windows Server 2003 中，__(46)__组成员用户具有完全控制权限。(2016 年下半年真题 46)

A. Users　　B. Power　Users　　C. Administrators　　D. Guests

解析：Administrators(管理员)组成员用户具有完全控制权限。

答案：C

例 9-12 在 Windows 的 DOS 窗口中输入以下命令：

```
C:\>nslookup
＞settype=ptr
＞211.151. 91.165
```

这个命令序列的作用是__(50)__。(2016 年上半年真题 50)

A. 查询 211.151. 91.165 的邮件服务器信息

B. 查询 211.151. 91.165 到域名的映射

C. 查询 211.151. 91.165 的资源记录类型

D. 显示 211.151. 91.165 中各种可用的信息资源记录

解析：PTR 记录也被称为指针记录。PTR 记录是 A 记录的逆向记录，作用是把 IP 地址解析为域名。

答案：B

例 9-13 下图是配置某邮件客户端的界面，图中 a 处应填写__(39)__，b 处应填写__(40)__。(2015 年下半年真题 39、40)

(39) A. abc.com　　B. POP3.abc.com
　　C. POP.com　　D. POP3.com

(40) A. 25　　B. 52　　C. 100　　D. 110

解析：由图中 SMTP 服务器的域名 SMTP.abc.com 知道，邮件服务器所在主机的主机名为 abc.com，而接收服务器类型为 POP3，因此空 a 填入 POP3.abc.com。在 TCP/IP 下，POP3 分配的端口号为 110，因此空 b 填入 110。

答案：(39) B　(40) D

9.3.3　同步练习

1. 以下关于 Windows Server 2003 域管理模式的描述中，正确的是________。
   A. 域间信任关系只能是单向信任
   B. 单域模型中只有一个主域控制器，其他都为备份域控制器
   C. 如果域控制器改变目录信息，应把变化的信息复制到其他域控制器
   D. 只有一个域控制器可以改变目录信息

2. 在 Windows Server 2003 环境中有本地用户和区域用户两种，其中本地用户信息存储在________。
   A. 本地计算机的 SAM 数据库　　B. 本地计算机的活动目录
   C. 域控制器的活动目录　　D. 域控制器的 SAM 数据库

9.3.4　同步练习参考答案

1. C　　2. A

9.4　Linux Apache 服务器的配置

9.4.1　考点辅导

9.4.1.1　Apache 的安装和配置

在 Webmin 的 system 页，选择 Software Packages，在该页 Install a New Package 中，

选择 From uploaded file，从上载文件安装，如：路径为 e:\RedHat\RPMS\apache，单击“浏览”按钮，指定要安装的包文件 Apache-1.3.23-11.i386.rpm，单击 Install 按钮即可。

1. Apache 的启动与停止

在 Apache Webserver 页操作：

(1) 在 Apache Webserver 页的上页标中，选择 Start Apache 来启动 Apache 服务器。

(2) Apache 服务器启动后，Apache Webserver 选项卡的上页标项有所变化，原 Start Apache 变为 Apply Changes 和 Stop Apache。在上页标中，选择 Stop Apache 来停止 Apache 服务器。

在 Bootup and Shutdown 页操作：

(1) Bootup and Shutdown 页中，在守护进程列表中查找 httpd，这是 Apache 服务器的守护进程名称，选中守护进程名称前的复选框，以选定此服务。

(2) 守护进程列表的下方有 Start Selected 和 Stop Selected 两个按钮，分别用来启动和停止选定的服务。

(3) 如在守护进程列表中直接选择守护进程 httpd，打开 Edit Actions 选项卡，显示服务器守护进程的详细配置信息，如守护进程的启动脚本。

2. Apache 的配置界面

在 Apache Webserver 选项卡中，界面配置的第一部分为 Global Configuration，包含若干全局设置项，全局设置项中的设置将作用于整个 Apache 服务器。

在 Apache Webserver 选项卡中，界面配置的第二部分为 Virtual Servers，显示当前服务器中的所有虚拟主机，在未进行配置的情况下包括两个虚拟主机，一个是 Default Server 默认主机，另一个是虚拟主机，使用 HTTPs，监听端口为 443，文档根目录 Document Root 与默认主机相同。

在 Apache Webserver 选项卡中，界面配置的第三部分为 Create a New Virtual Server，此对话框用于建立一个新的虚拟主机。

9.4.1.2 建立基于域名的虚拟主机

虚拟主机服务是指在一台物理机器上提供多个 Web 服务。例如，某公司有多个子公司，各子公司需要拥有独立的域名，希望对外提供独立的 Web 服务，但是都要使用总公司的单台服务器。这时该服务器就通过虚拟主机的方式，为各个子公司提供多个企业的 Web 服务。虽然所有的 Web 服务都是这台服务器提供的，但是让访问者看起来却像在不同的服务器上获得 Web 服务一样。

用 Apache 设置虚拟主机服务通常可以采用两种方案：基于 IP 地址的虚拟主机和基于域名的虚拟主机。

基于域名的虚拟主机服务是目前应用比较广泛的一种方案。它不需要更多的 IP 地址，而且配置简单，无须特殊的软、硬件支持。现在的浏览器大都支持这种虚拟主机的实现方法。

在 Create a New Virtual Server 对话框中配置需要建立的主机，address 设置为当前主机的某个 IP 地址，如 192.168.1.112，并选中 Add name virtual server address 和 Listen on address；

Prot 为 Default；Document Root 设置为此虚拟主机的文档根目录，如/var/www/page.test.com，此目录是在配置 wu-ftpd 服务器时为虚拟站点 page.test.com 建立的；Server Name 设置为此虚拟主机的域名，如 page.test.com；Add virtual server to file 选取 standardhttpd.conf 文件，单击 Create 按钮，建立已配置完成的虚拟服务器。

刚刚建立的虚拟服务器虽然已经保存到 Apache 的配置文件中，但并未生效，需要选择 Apache Webserver 选项卡的 Apply Changes，使已修改的配置生效。

需要在 test.com 的授权 DNS 中注册 IP 地址 192.168.1.112，指向虚拟主机的域名 page.test.com；Name 为 page；Update 为 Yes；Time-to-Live 为 Default。

9.4.1.3　建立基于 IP 地址的虚拟主机

基于 IP 地址的虚拟主机服务实现需要在机器上配置多个 IP 地址。每个 IP 地址对应一个虚拟主机。这种方法需要每个虚拟主机占用一个 IP 地址资源，在当前 IP 地址资源比较紧张的情况下很少使用这种方法。

1. 为网卡绑定多个 IP 地址

为网卡绑定多个 IP 地址的具体操作如下。

(1) 在 Hardware 选项卡中，选择 Network Configuration，在该页中选择 Network Interfaces。在 Network Interfaces 页中，Interfaces Active Now 列表显示了当前系统激活网卡的信息，如名称为 eth0 的网卡类型为 Ethernet；分配的 IP 地址为 192.168.1.112；掩码(Netmaskw)为 257-257-257-0；状态(Status)为 Up。选择 Add a new interface，添加新的接口。

(2) 在 Create Active interface 选项卡中，配置要建立的网卡，Name 设为 eth0:0 表示这并不是一块真正的网卡，而是指向物理网卡 eth0 的一个虚拟网卡；192.168.1.113 为给 eth0 绑定的另一个 IP 地址；其他设置为默认选项；单击 Create 按钮，建立已配置好的网卡。

(3) Network Interfaces 选项卡中，Interfaces Active Now 列表已经显示了新建立的网卡 eth0:0，类型 Ethernet(Virtual)表示其为虚拟以太网卡。

2. 建立基于 IP 地址的虚拟主机的步骤

建立基于 IP 地址的虚拟主机的具体操作如下。

(1) 在 Create a New Virtual Server 对话框中，配置要建立的主机，Address 设置为要建立虚拟主机的 IP 地址，如 192.168.1.113，并选取 Add name virtual server address 和 Listen on address；Port 的 Default 设置为“80”；设置 Document Root 为/var/www/ip.test.com；设置 Server Name 为 ip.test.com；Add virtual server to file 选取 Standard httpd.conf file；单击 Create 按钮，建立已配置完成的虚拟服务器。

(2) 选择 Apache Webserver 选项卡的 Apply Changes，使已修改的配置生效。

(3) 需要在 test.com 的授权 DNS 中注册 IP 地址 192.168.1.113 指向虚拟主机域名 ip.test.com；Name 为 ip；Update 为 Yes；Time-to-Live 为 Default。

9.4.1.4　Apache 中的访问控制

Web 网站常有这样的需要，对网站某部分内容进行简单的密码保护，只允许授权的用户访问。例如，网站的统计分析结果不允许普通用户随意浏览。Apache 提供了基于用户名/口令的认证方式以满足这样的需求。

Apache 实现身份认证的基本原理是，当系统管理员需要对某个目录设置身份认证时，就在要限制的目录中添加默认名为.htaccess 的配置文件。当用户访问该路径下的资源时，系统就会弹出一个对话框，要求用户输入“用户名/口令”。用户输入口令后，传给 WWW 服务器。WWW 服务器将验证它的正确性，如果正确，则返回页面；否则返回 401 错误。要说明的一点是，这种认证模式不能用于安全性要求很高的场合。

下面来看一下如何建立需要用户名/口令才能进行访问的目录。假设基本情况是，www.domainname.com 站点的文档存放在/var/www/html 目录下，而 Web 访问日志分析存放在/var/www/usage 目录下，希望限制/var/www/usage/目录的访问，只允许用户 admin 以口令 passkey 访问该目录。

首先确保在 Apache 的 httpd.conf 中，用密码才能访问的目录或其父目录的 Directory 容器的设置参数中包含以下设置：

```
AllowOverride All
```

或

```
AllowOverride AuthConfig
```

即允许该目录对 Authconfig 属性进行覆盖。

然后使用 htpasswd 命令建立用户文件、账号信息文件：

```
htpasswd-c /etc/.htpasswd admin
```

上述代码创建了名为.htpasswd 的用户账号文件，并初始化一个 admin 用户。此程序会询问用户 admin 的口令，两次输入 passkey 即可完成。

在希望限制访问的目录(这里为/var/www/usage/)下建立.htaccess 文件，用 vi 在/var/www/usage/目录下创建文件.htaccess：

```
AuthName Administrator Accessible Only    /*这个名字是任意取的*/
AuthType Basic
AuthUserFile /etc/.htpasswd
require user admim
```

9.4.2 典型例题分析

例 9-14 在 Linux 系统中，使用 Apache 服务器时默认的 Web 根目录是__(35)__。(2016 年上半年真题 35)

A. ..\htdocs　　B. /var/www/html　　C. /var/www/usage　　D. ..\conf

解析：Apache HTTP Server(简称 Apache)是 Apache 软件基金会的一个开放源代码的网页服务器，可以在大多数计算机操作系统中运行，由于其多平台和安全性被广泛应用，是最流行的 Web 服务器端软件之一。在 Linux 中，使用 Apache 服务器时默认的 Web 根目录是/var/www/html。

答案：B

例 9-15 下面关于 Linux 系统文件挂载的叙述中，正确的是__(36)__。(2016 年上半年真题 36)

A. /可以作为一个挂载点

B. 挂载点可以是一个目录，也可以是一个文件

C. 不能对一个磁盘分区进行挂载

D. 挂载点是一个目录时，这个目录必须为空

解析：挂载点必须是一个目录。一个分区挂载在一个已存在的目录上，这个目录不为空，但挂载后这个目录下以前的内容将不可用。/根目录：存放系统命令和用户数据等(如果下面的挂载点没有单独的分区，它们都将在根目录的分区中)。

答案：A

9.4.3　同步练习

1. 在一台 Apache 服务器上通过虚拟主机可以实现多个 Web 站点。虚拟主机可以是基于＿(1)＿的虚拟主机，也可以是基于名字的虚拟主机。若某公司创建名字为 www.business.com 的虚拟主机，则需要在＿(2)＿服务器中添加地址记录。在 Linux 中该地址记录的配置信息如下，请补充完整。

```
        NameVirtualHost  192.168.0.1
<VirtualHost  192.168.0.1>
 (3)  www.business.com
  DocumentRoot  /var/www/html/business
</VirtualHost>
```

(1) A. IP　B. TCP　C. UDP　D. HTTP

(2) A. SNMP　B. DNS　C. SMTP　D. FTP

(3) A. WebName　B. HostName　C. ServerName　D. WWW

2. Linux 操作系统中，网络管理员可以通过修改＿＿＿＿文件对 Web 服务器端口进行配置。

A. inetd.conf　B. lilo.conf　C. httpd.conf　D. resolv.conf

3. Linux 操作系统中，建立动态路由器需要用到文件＿＿＿＿。

A. /etc/inetd.conf　B. /etc/lilo.conf

C. /etc/httpd/conf/httpd.conf　D. /etc/httpd/conf/access.conf

9.4.4　同步练习参考答案

1. (1) A　(2) B　(3) C　2. C　3. C

9.5　DNS 服务器的配置

9.5.1　考点辅导

9.5.1.1　DNS 服务器基础

Internet 上的主机用 IP 地址进行识别，但通常都使用主机名，因为主机名便于记忆并且易于被人们接受。由主机名到 IP 地址的转换过程被称为名称解析。完成动态名称解析的系

统称为 DNS (Domain Name System，域名系统)。

域名服务器分为以下 4 种。

(1) 主域名服务器：负责维护这个区域的所有域名信息，是特定域的所有信息的权威信息源。也就是说，主域名服务器内所存储的是该区域的正本数据，系统管理员可以对它进行修改。

(2) 辅助域名服务器：当主域名服务器出现故障、关闭或负载过重时，辅助域名服务器作为备份服务器提供域名解析服务。辅助域名服务器中的区域文件内的数据是从另外一台域名服务器复制过来的，并不是直接输入的。也就是说，这个区域文件的数据只是一份副本，这里的数据是无法修改的。

(3) 缓存域名服务器：可运行域名服务器软件但没有域名数据库。它从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。缓存域名服务器是不权威性服务器，因为它提供的所有信息都是间接信息。

(4) 转发域名服务器：负责所有非本地域名的本地查询。转发域名服务器接到查询请求时，在其缓存中查找，如果找不到就把请求依次转发到指定的域名服务器，直到查询到结果为止，否则返回无法映射的结果。

9.5.1.2 Windows Server 2008 R2 DNS 服务器的安装与配置

1. 安装 DNS 服务器

Windows Server 2008 R2 系统内置了 DNS 服务组件，但默认情况下并没有安装，需要管理员手动安装并配置，从而为网络提供域名解析服务。

在一台运行 Windows Server 2008 R2 的计算机上安装 DNS 服务器的操作步骤如下。

(1) 选择“开始”→“管理工具”→“服务器管理器”→“角色”命令，在打开的窗口中单击“添加角色”按钮，启动 Windows 添加角色向导。

(2) 在“服务器角色”列表框中勾选“DNS 服务器”复选框，并单击“下一步”按钮。按照向导提示，执行至确认界面，单击“安装”按钮完成 DNS 服务器的安装。

2. 设置 DNS 服务器

安装完 DNS 服务器后，需要对其进行设置，这样 DNS 服务器才能为客户机提供服务。用于配置和管理 Windows Server 2008 R2 DNS 服务器的主要工具是 DNS 控制台 dnsmgmt。

从“管理工具”窗口中单击 DNS，可以看出 DNS 控制台已默认将本地服务器列在控制台左侧的树中。

假设局域网的域名为 example.com，其中有一台主机作为 WWW 服务器，IP 地址为 192.168.1.30，按照惯例将这台主机命名为 www.example.com。下面介绍如何在 DNS 服务器中实现对该主机名称的解析，步骤如下。

(1) 首先在 DNS 服务器中新建一个名为 example.com 的区域。右键单击控制台目录树中的 EX-WIN2008SVR 服务器，在弹出的快捷菜单中选择“配置 DNS 服务器”命令，打开“配置 DNS 服务器向导”对话框，单击“下一步”按钮。

(2) 在“选择配置操作”对话框中，为了简化 DNS 服务器的配置，选择“创建正向和反向查找区域”，单击“下一步”按钮。

提示：正向查找区域用于进行 DNS 正向查询，即允许客户端通过已知的主机名，查找其所对应的 IP 地址；反向查找区域用于进行 DNS 反向查询，即允许客户端使用已知的 IP 地址，查找其所对应的计算机名。

(3) 在“新建区域向导”对话框中，由于此时配置的是网络内的第一台 DNS 服务器，所以选中“创建主要区域”单选按钮，单击“下一步”按钮。

(4) 在“区域名称”文本框中输入区域的名称 example.com，如图 9-22 所示，单击“下一步”按钮。

(5) 在“区域文件”向导页中，选中“创建新文件，文件名为”单选按钮，并使用系统默认的文件名 example.com.dns，单击“下一步”按钮，如图 9-23 所示。

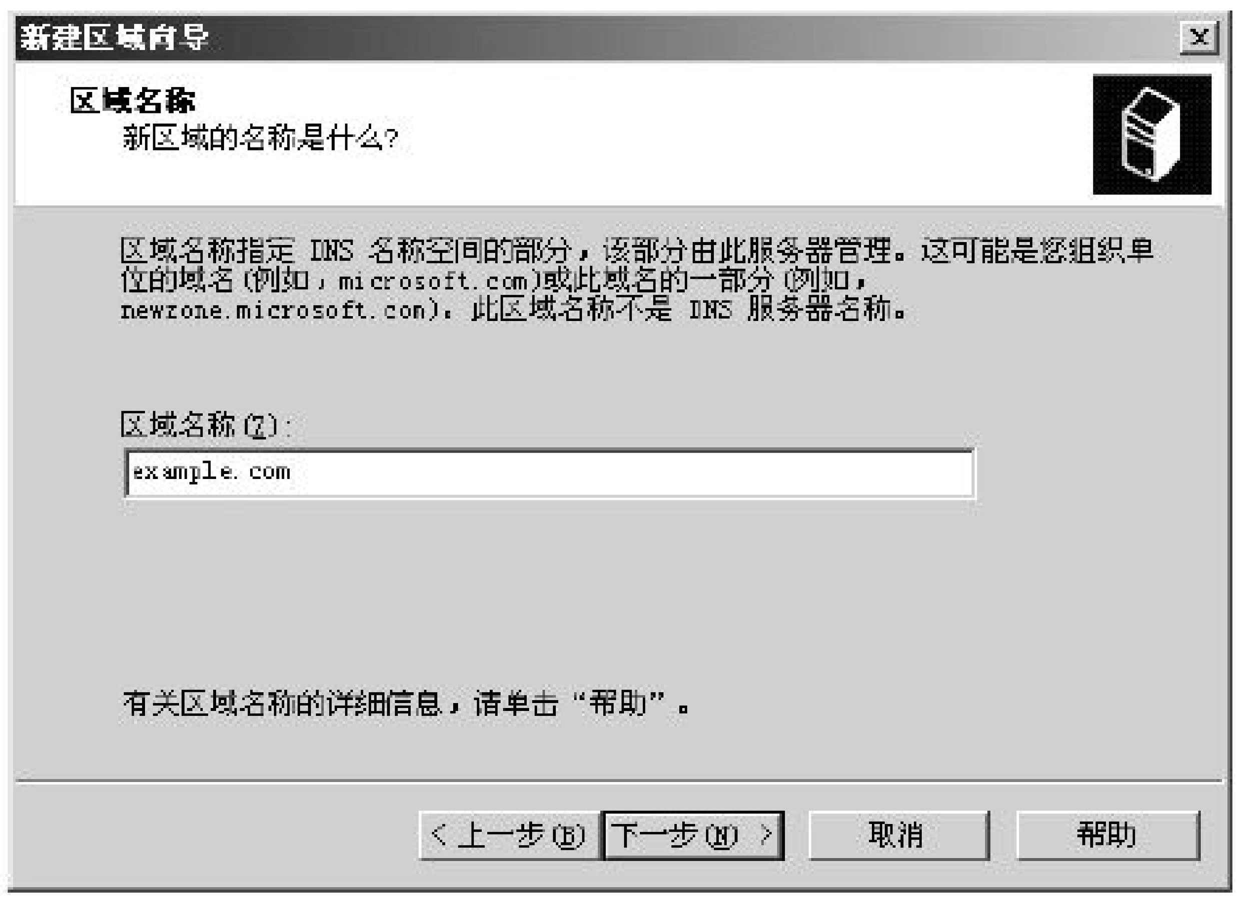


图 9-22　输入区域名称

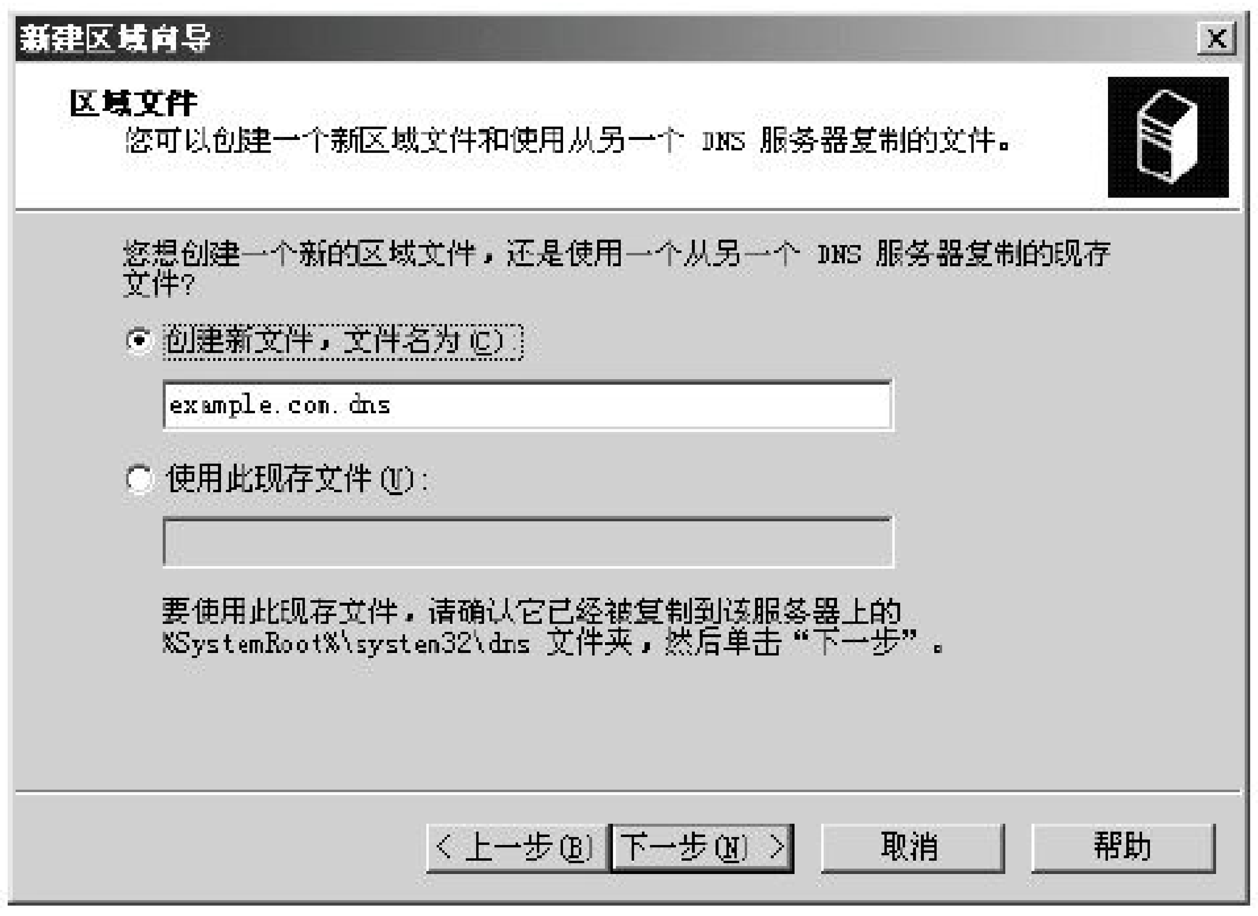


图 9-23　创建新的区域文件

(6) 在“动态更新”向导页中，选中“不允许动态更新”单选按钮，如果服务器已安装了 Active Directory，也可以选中“只允许安全的动态更新”单选按钮，以便最大限度地集成和支持 Active Directory 以及增强 DNS 服务器功能。单击“下一步”按钮，如图 9-24 所示。

(7) 接下来配置反向区域，在“反向查找区域”向导页中，选中“是，现在创建反向查找区域”单选按钮，单击“下一步”按钮。在接下来的“区域类型”向导页中，依旧选中“主要区域”单选按钮，再单击“下一步”按钮。

(8) 在“反向查找区域名称” 向导页中，选中“网络 ID”单选按钮，并在下面输入本网络的网络 ID，如 192.168.1，如图 9-25 所示，单击“下一步”按钮。

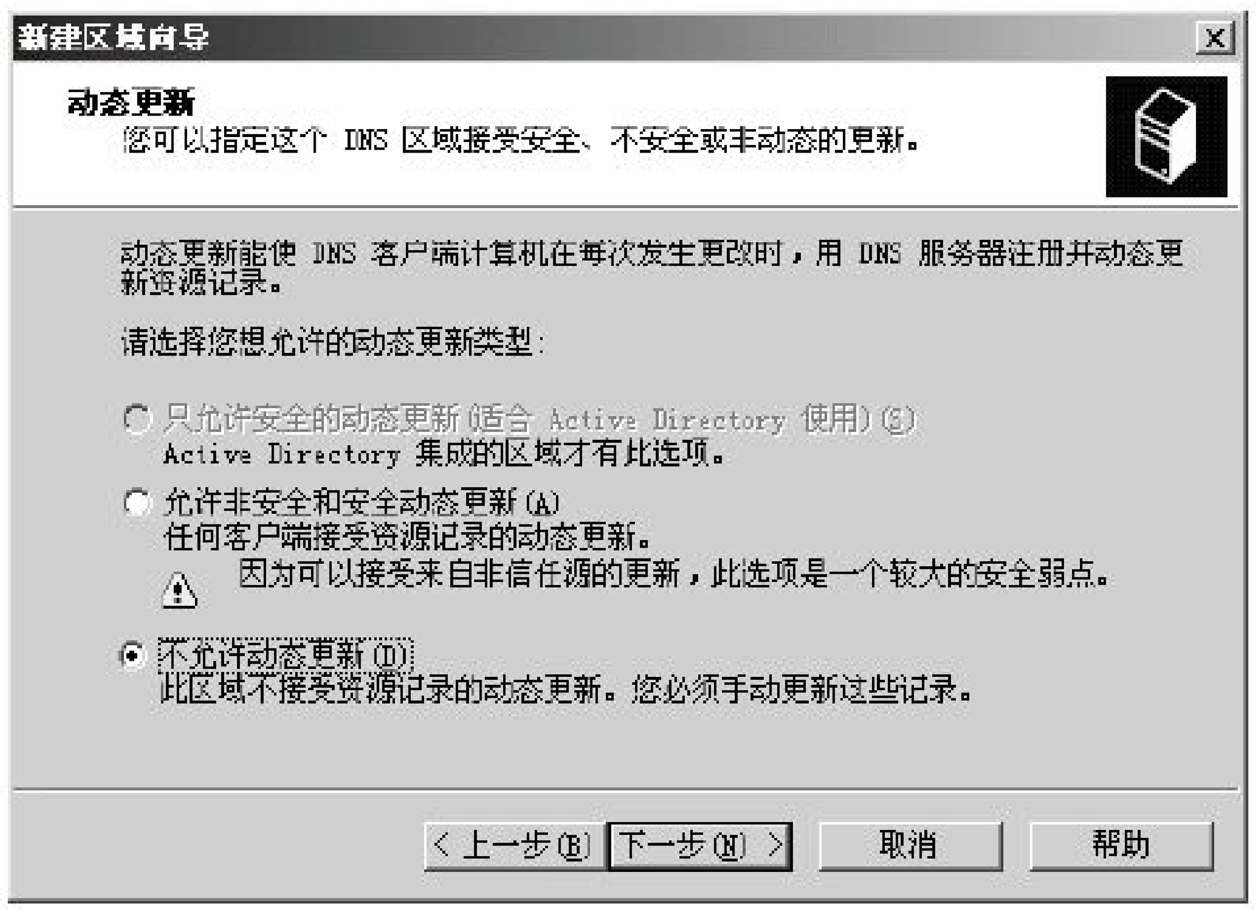


图 9-24　设置 DNS 服务器动态更新类型

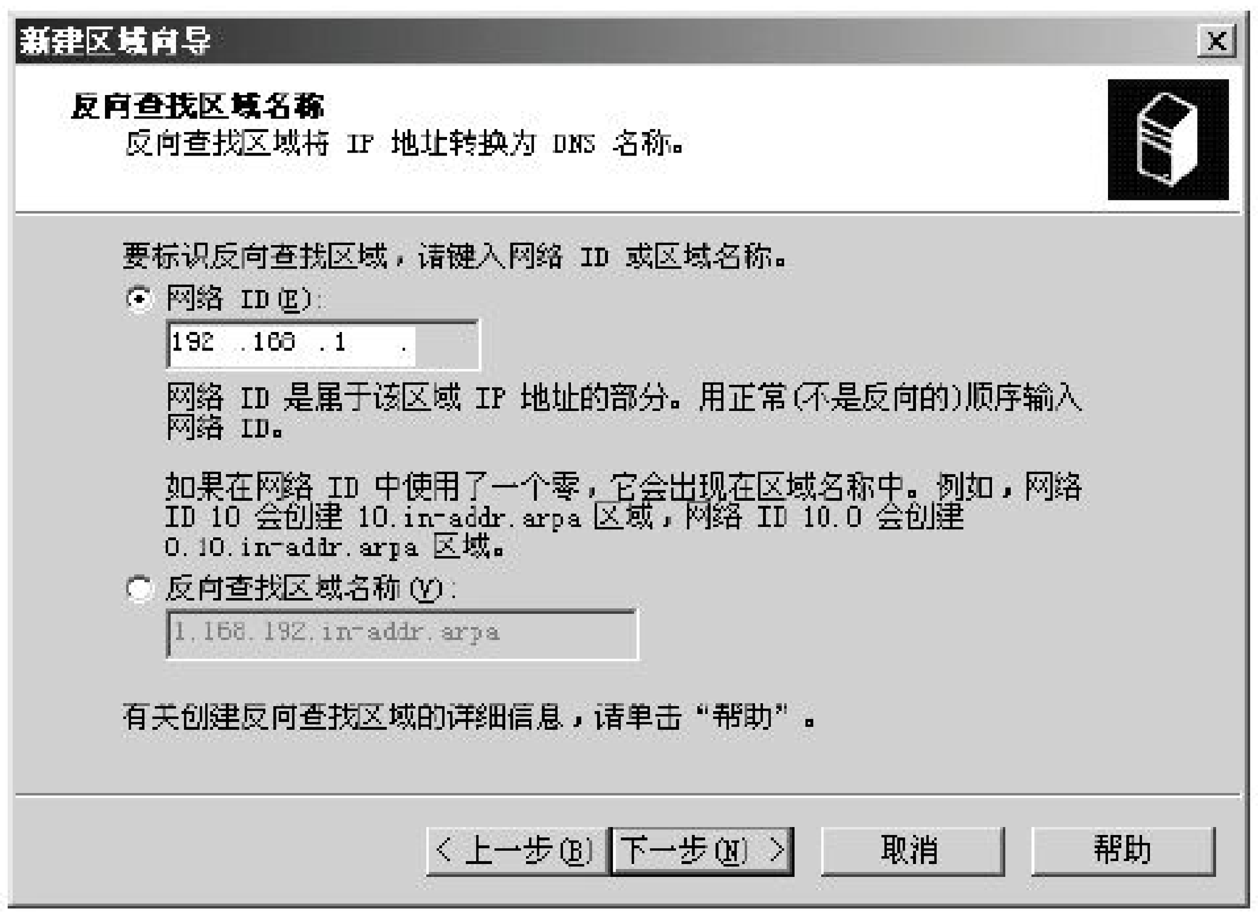


图 9-25　设置反向查找区域名称

(9) 在接下来的“区域文件”和“动态更新”两个向导页中，分别选中“创建新文件，文件名为”和“不允许动态更新”单选按钮，文件名按照系统默认给出。

(10) 在“转发器”向导页中，暂时选中“否，不向前转发查询”单选按钮。转发器的具体用途和配置方法后面会做进一步介绍。单击“下一步”按钮，如果配置顺利，会弹出一个对话框，提示已成功地完成了 DNS 服务器配置向导，单击“确定”按钮关闭对话框。

DNS 服务器配置完成后，在控制台的目录树中可以看到，服务器节点下建立了“正向查找区域”和“反向查找区域”。双击展开“正向查找区域”，会看到新区域 example.com 已经添加。单击 example.com，右半窗口中会显示该区域的配置信息。

3. 创建域名

下面介绍如何建立主机 www.example.com，其操作步骤如下。

(1) 依次选择“开始”→“管理工具”→DNS 命令，打开 dnsmagt 控制台窗口。

(2) 在左窗格中依次展开 ServerName→“正向查找区域”目录，然后用鼠标右击区域名处，从弹出的快捷菜单中选择“新建主机”命令，弹出如图 9-26 所示的对话框，输入主机名 www，IP 地址 192.168.1.30。

(3) 如果希望 DNS 服务器也能够进行反向查询，则选中“创建相关指针(PTR)记录”复选框，单击“添加主机”按钮。如果添加成功，系统会提示“成功地创建了主机记录 example.com。”，如图 9-27 所示，单击“确定”按钮。

(4) 如果不再添加主机，单击“完成”按钮。

图 9-26 “新建主机”对话框

图 9-27 主机记录创建成功

4. 安装客户端

安装 DNS 客户机的步骤如下。

(1) 在“控制面板”对话框中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，在打开的“本地连接 属性”对话框中选中“Internet 协议(TCP/IP)”复选框，单击“属性”按钮，打开如图 9-28 所示的对话框。

(4) 在图 9-28 的“首选 DNS 服务器”文本框中输入一台 DNS 服务器的 IP 地址，然后

单击“确定”按钮，这样便把该计算机配置为那台 DNS 服务器的 DNS 客户机了。

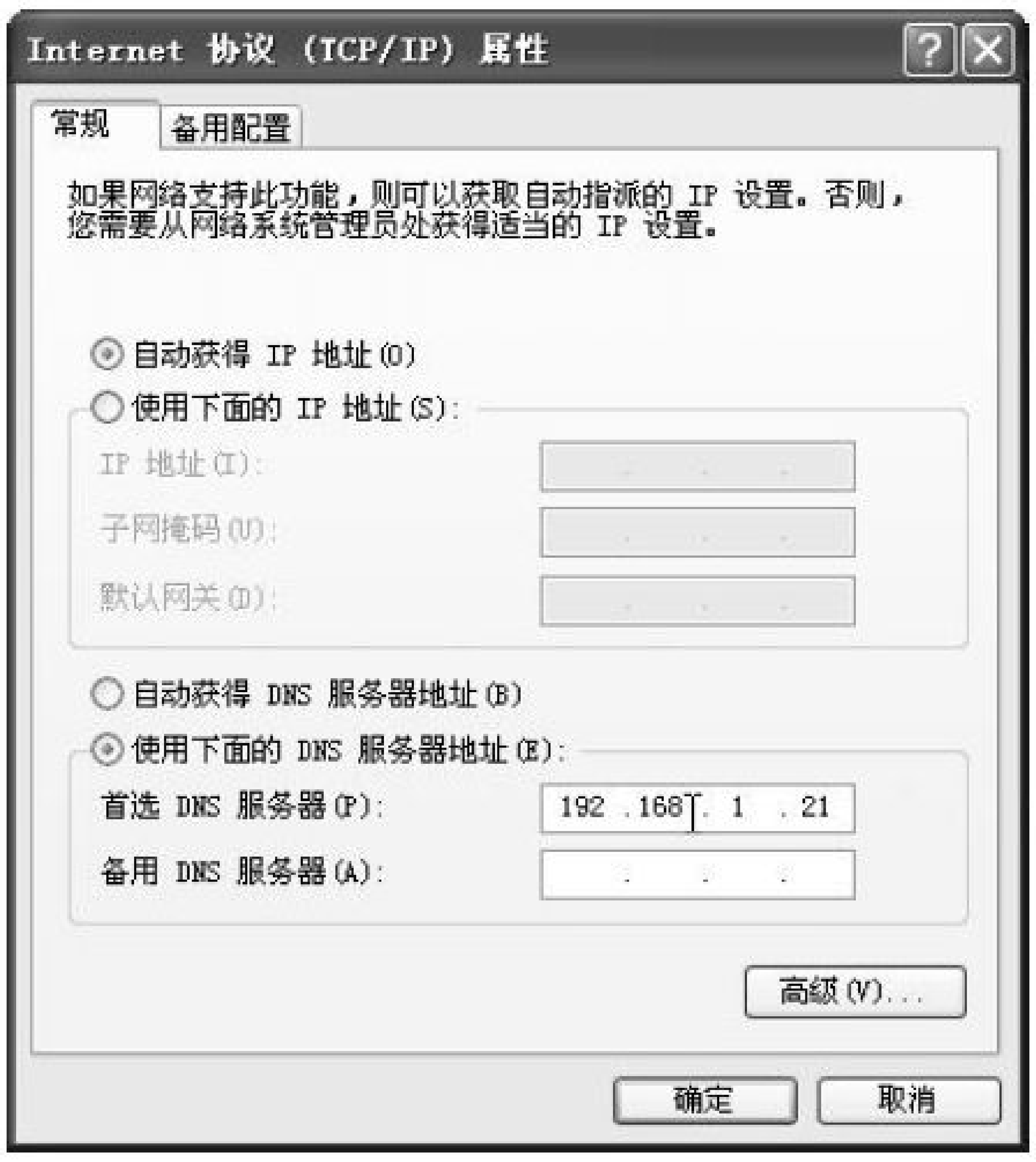


图 9-28　“Internet 协议(TCP/IP)属性”对话框

9.5.1.3　Linux BIND DNS 服务器的安装

安装 bind 软件包，可使用“本地文件”“上载文件”和网络站点(FTP、HTTP 和 RedHat Network)等多种方法，双击\RedHat\RPMS\bind-9.2.0-8.i386.rpm 文件打开安装界面。

1. 配置 DNS 解析器

在 Linux 主机上使用 Webmin 管理工具配置 DNS 客户端。通过浏览器登录 Linux 主机的 Webmin 界面。在“硬件”页中，选择“网络配置”项。在“网络配置”页中，选择“DNS 客户”项。在“DNS 服务器”项输入要使用的 DNS 域名服务器的 IP 地址，如 192.168.1.114，最多可以输入 3 个 DNS 的 IP 地址，DNS 查询时将按先后顺序分别查询；设置解析顺序为“DNS”“Hosts”，表示先查询 DNS 服务器再查询本地 Hosts 文件。

2. 高速缓存服务器的配置

通过浏览器登录 Linux 主机的 Webmin 界面，选择“服务”页，选择“BIND DNS 服务器”。

BIND DNS 服务器的所有配置都可在“BIND DNS 服务器”界面完成。

BIND 默认安装已存在 Root 区、129.0.0 和 localhost 区。在“现有 DNS 区域”部分可看到这 3 项。

BIND 默认安装情况下可直接作为高速缓存服务器，只需单击“启动名字服务器”按钮，启动 BIND 服务器即可。

3. 主服务器的配置

正向主服务器的区域类型为“正向”，即名称至地址的正向解析。

反向主服务器的区域类型为“反向”，即地址至名称的反向解析。

新建正向主服务器，在“新建主区域”页，“区域类型”默认选项为“正向(名称至地址)”；“域名/网络”项填入要新建的主区域域名。

新建反向主服务器，在“新建主区域”页，“区域类型”默认选项为“反向(地址至名称)”；“域名/网络”项填入要反向解析的网络地址。

在正向主服务器中增加地址记录。

在正向主服务器中增加名称别名记录。

在正向主服务器中增加邮件交换记录。

在正向主服务器中增加 slave 名称服务器记录。查看主服务器的正向、反向区域，并使设置生效。

4. 从服务器的配置

建立次服务器的正向解析，在“新建次区域”页中进行配置，“区域类型”默认为“正向解析”；在“域名/网络”项输入要作为哪个域的从服务器。

核实“编辑次区域”页的“区域选项”，“主服务器”IP 地址为 192.168.1.114，是在“新建次区域”页中输入的，“记录文件”为自动生成的全路径记录文件名/var/named/test.com.hosts，文件名根据当前域名生成，其他项为默认值；单击“保存”按钮，保存当前设置。

建立次服务器反向解析，在“新建次区域”页将“区域类型”设为“反向解析”；“域名/网络”为域名的网络地址 192.168.1。

选择区域可以对该区域的属性进行编辑，修改后保存，也可以把次区域转换成主区域，单击 Conver to master zone 按钮，即可实现。

5. DNS 的测试

以超级用户权限登录，使用 nslookup 命令对 BIND DNS 服务器进行测试。

```
#nslookup
>master.test.com /*测试正向解析地址记录，查询主机 master.test.com 的 IP 地址*/
Server: 192.168.1.114
Address: 192.168.1.114#53
Name: master.test.com
Address: 192.168.1.114
>192.168.1.113/*测试反向解析地址记录，查询 IP 地址为 192.168.1.113 的主机名称*/
Server: 192.168.1.114
Address: 192.168.1.114#53
113.1.168.192.in-addr.arpa name=slave.test.com
>dns.test.com/*测试“名称别名”记录，查询主机 dns.test.com 的别名*/
Server: 192.168.1.114
Address: 192.168.1.114#53
dns.test.com canonical name=master.test.com
Name: master.test.com
Address: 192.168.1.114>set type = ns/*测试 type 为“NS”(Name Server 名称服务
器)的记录*/
>test.com
Server: 192.168.1.114
Address: 192.168.1.114#53
test.com: nameserver = slave.test.com
```

```
test.com: nameserver = master.test.com
>set type = mx/*测试类型为“MX”(Mail Exchanger，邮件服务器)的记录*/
>test.com
Server: 192.168.1.114
Address: 192.168.1.114#53
test.com: mail exchanger = 10 mail.test.com
```

9.5.2　典型例题分析

例 9-16　在进行域名解析的过程中，若主域名服务器发生故障，由转发域名服务器传回解析结果，下列说法中正确的是__(34)__。(2017 年下半年真题 34)

A. 辅助域名服务器配置了递归算法　　B. 辅助域名服务器配置了迭代算法

C. 转发域名服务器配置了递归算法　　D. 转发域名服务器配置了迭代算法

解析：通常本地 DNS 服务器使用递归形式查询，除此之外，转发域名服务器也使用递归算法。

答案：C

例 9-17　在 DNS 资源记录中，__(35)__记录类型的功能是实现域名与其别名的关联。(2017 年下半年真题 35)

A. MX　　B. NS　　C. CNAME　　D. PTR

解析：CNAME 实现别名记录，实现同一台服务器可提供多种服务。

答案：C

例 9-18　在运行 Windows Server 2003 R2 的 DNS 服务器上要实现 IP 地址到主机名的映射，应建立__(37)__记录。(2017 年下半年真题 37)

A. 指针 (PTR)A　　B. 主机信息 (HINFO)

C. 服务位置(SRV)　　D. 规范名称 (CNAME)

解析：实现 IP 地址到主机名的映射，是一种与域名到 IP 地址相反的映射，使用指针实现。

答案：A

9.5.3　同步练习

1.　在 Windows 系统中可通过停止________服务器来阻止对域名解析 Cache 的访问。

A. DNS Server　　B. Remote Procedure　　C. Ns Lookup　　D. DNS Client

2.　在 Linux 操作系统中，采用________来搭建 DNS 服务器。

A. Samble　　B. Tomcat　　C. Bind　　D. Apache

3.　在 Windows Server 2003 的 DNS 服务器中通过________操作，实现多台 Web 服务器构成集群并共享同一域名。

A. 启用循环(Round Robin)，添加每个 Web 服务器的主机记录

B. 禁止循环(Round Robin)，启动转发器指向每个 Web 服务器

C. 启用循环(Round Robin)，启动转发器指向每个 Web 服务器

D. 禁止循环(Round Robin)，添加每个 Web 服务器的主机记录

4. 下面有关 DNS 的说法中错误的是______。

A. 主域名服务器运行域名服务器软件，有域名数据库

B. 辅助域名服务器运行域名服务器软件，但是没有域名数据库

C. 转发域名服务器负责本地域名的本地查询

D. 一个域有且只有一个主域名服务器

5. 下图所示是在 Windows 客户端 DOS 窗口中使用 nslookup 命令后的结果，该客户端的首选 DNS 服务器的 IP 地址是__(1)__。在 DNS 服务器中，ftp.test.com 是采用新建__(2)__的方式建立的。

```
C:\Documents and Settings\user>nslookup  score.test.com
Server：  ns1.test.com
Address：  192.168.21.252

Non-authoritative answer：
Name:     score.test.com
Address：  10.10.20.3

C:\Documents and Settings\user>nslookup  ftp.test.com
Server：  ns1.test.com
Address：  192.168.21.252

Non-authoritative answer：
Name：   ns1.test.com
Address：  10.10.20.1
Aliases：  ftp.test.com
```

(1) A. 192.168.21.252　　B. 10.10.20.3

C. 10.10.20.1　　D. 以上都不是

(2) A. 邮件交换器　　B. 别名　　C. 域　　D. 主机

9.5.4 同步练习参考答案

1. D　　2. C　　3. A　　4. B　　5. (1) A　(2) B

9.6 DHCP 服务器的配置

9.6.1 考点辅导

9.6.1.1 DHCP 服务器基础

在常见的小型网络中，IP 地址的分配一般采用静态方式，但在大中型网络中，为每一台计算机分配一个静态 IP 地址，将加重网管人员的负担，并且容易导致 IP 地址分配错误。因此，在大中型网络中使用 DHCP (Dynamic Host Configuration Protocol，动态主机配置协议)服务是非常有效率的。DHCP 服务具有以下好处。

- 管理员可以迅速地验证 IP 地址和其他配置参数，而不用去检查每台主机。
- DHCP 服务不会从一个范围里同时租借相同的 IP 地址给两台主机，避免了手工操作的重复。

- 可以为每个 DHCP 范围(或者说所有的范围)设置若干选项(比如可以为每台计算机设置默认网关、DNS 和 WINS 服务器的地址)。
- 如果主机物理上被移动到了不同的子网上，该子网上的 DHCP 服务器将会自动用适当的 TCP/IP 配置信息重新配置该主机。
- 大大方便了便携机用户，移动到不同的子网上不再需要为便携机分配 IP 地址。

DHCP 服务的工作过程如下。

(1) 当 DHCP 客户机首次启动时，客户机向 DHCP 服务器发送一个 Dhcpdiscover 数据包，该数据包表达了客户机的 IP 租用请示。

(2) 当 DHCP 服务器接收到 Dhcpdiscover 数据包后，该服务器从地址范围中向那台主机提供(dhcpoffer)一个还没有被分配的有效的 IP 地址。当网络中包含不止一个 DHCP 服务器时，主机可能收到好几个 dhcpoffer，在大多数情况下，主机或客户机接收到第一个 dhcpoffer。

(3) 该 DHCP 服务器向客户机发送一个确认(dhcpack)，该确认里面已经包括了最初发送的 IP 地址和该地址的一个稳定期间的租约(默认情况是 8 天)。

(4) 当租约期过了一半时(即 4 天)，客户机将和设置它的 TCP/IP 配置的 DHCP 服务器更新租约。当租期过了 89.5%时，如果客户机仍然无法与当初的 DHCP 服务器联系上，它将与其他 DHCP 服务器通信，如果网络上再没有任何 DHCP 服务器在运行时，该客户机必须停止使用该 IP 地址，并从发送一个 dhcpdiscover 数据包开始，再一次重复整个过程。

9.6.1.2 Windows Server 2008 R2 DHCP 服务器的安装与配置

1. 安装 DHCP 服务器

Windows Server 2008 R2 系统内置了 DHCP 服务组件，但默认情况下并没有安装，需要管理员手动安装并配置，从而为网络提供 DHCP 服务。将一台运行 Windows Server 2008 R2 的计算机配置成 DHCP 服务器，最简单的方法是使用服务器管理器添加 DHCP 服务器角色，其过程如下。

(1) 通过“开始”菜单打开“服务器管理器”窗口，选择左侧的“角色”节点，单击“添加角色”超链接，启动添加角色向导。

(2) “开始之前”向导页中提示了此向导可以完成的工作，以及操作之前应注意的相关事项，单击“下一步”按钮继续。

(3) “选择服务器角色”向导页中显示了所有可以安装的服务器角色。如果角色前面的复选框没有被选中，则表示该网络服务尚未安装；如果已选中，则说明该服务已经安装。这里选中“DHCP 服务器”复选框，单击“下一步”按钮继续。

(4) “DHCP 服务器”向导页中对 DHCP 服务器的功能作了简要介绍，单击“下一步”按钮继续。

(5) 在“选择网络连接绑定”向导页中选择 DHCP 服务器将用于向客户端提供服务的网络连接，单击“下一步”按钮继续，如图 9-29 所示。

(6) 在“指定 IPv4 DNS 服务器设置”向导页中指定客户用于名称解析的父域名，以及客户端用于域名解析的 DNS 服务器 IP 地址，单击“下一步”按钮继续，如图 9-30 所示。

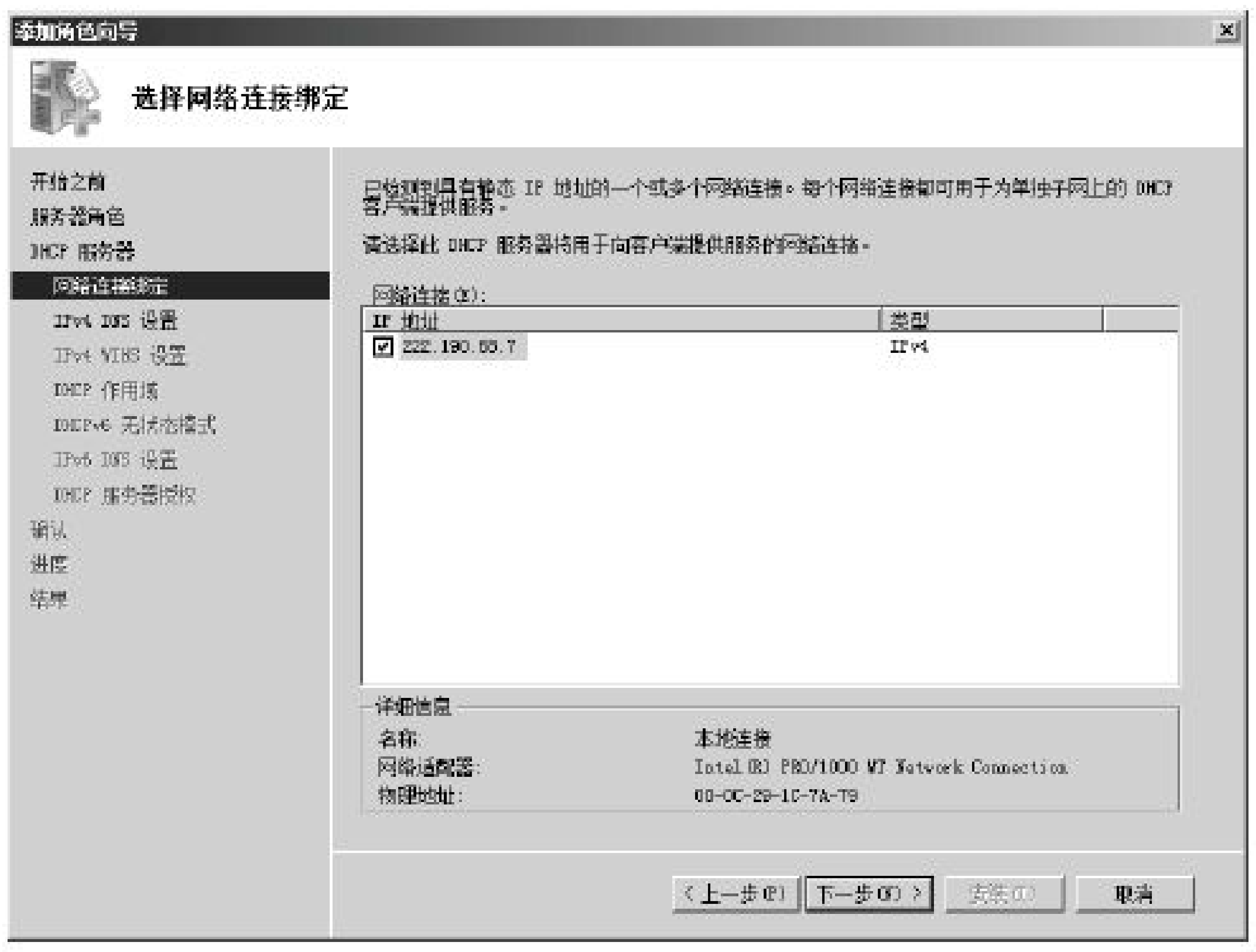


图 9-29 选择网络连接绑定

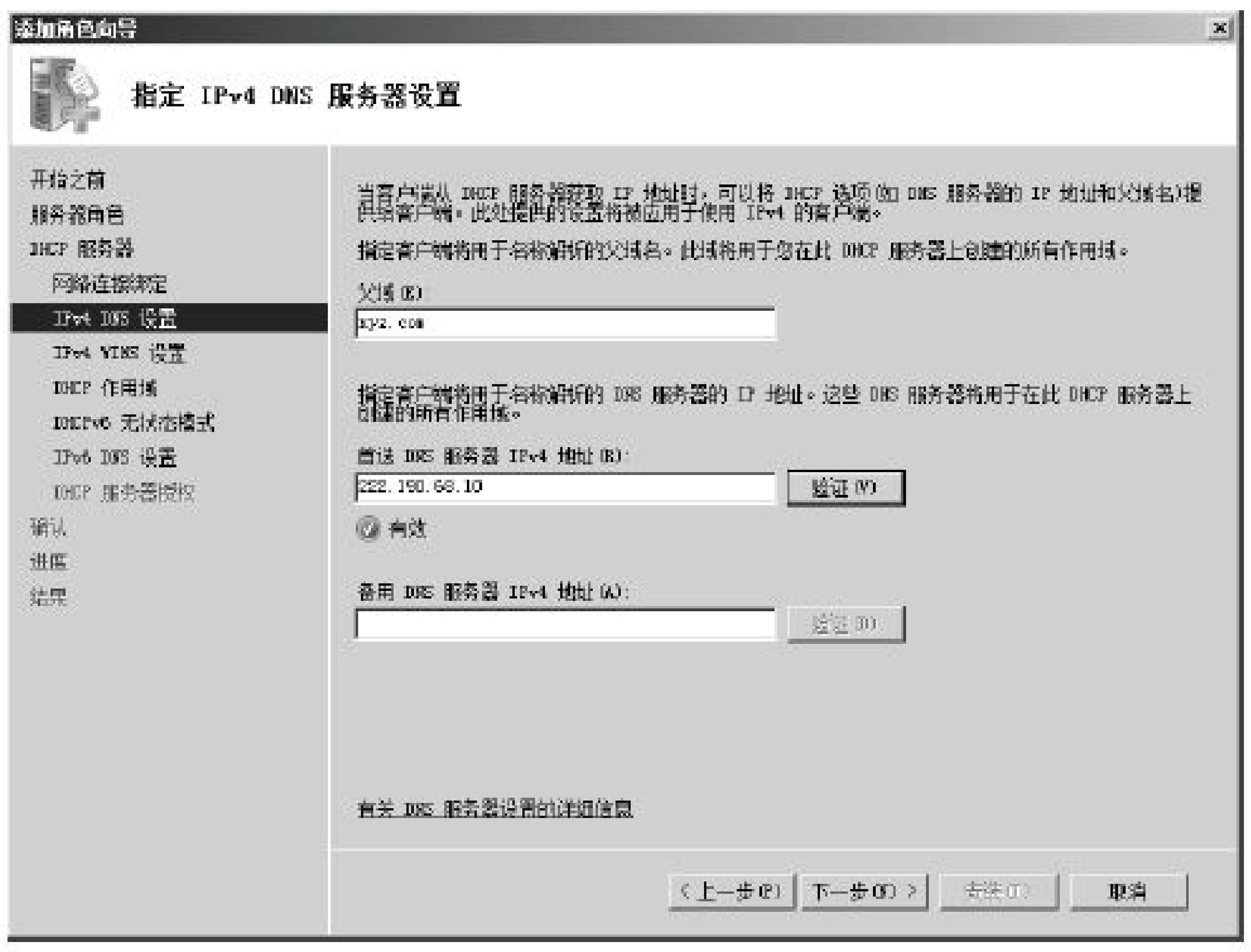


图 9-30 指定 IPv4 DNS 服务器设置(1)

(7) 在“指定 IPv4 WINS 服务器设置”向导页中选择是否使用 WINS 服务，单击“下一步”按钮继续，如图 9-31 所示。

(8) 在“添加或编辑 DHCP 作用域”向导页中可以添加 DHCP 作用域。只有指定了作用域，DHCP 服务器才能向客户端分配 IP 地址、子网掩码和默认网关等。现在可以不指定，等 DHCP 安装完成后再添加。若现在指定，可单击“添加”按钮，如图 9-32 所示。

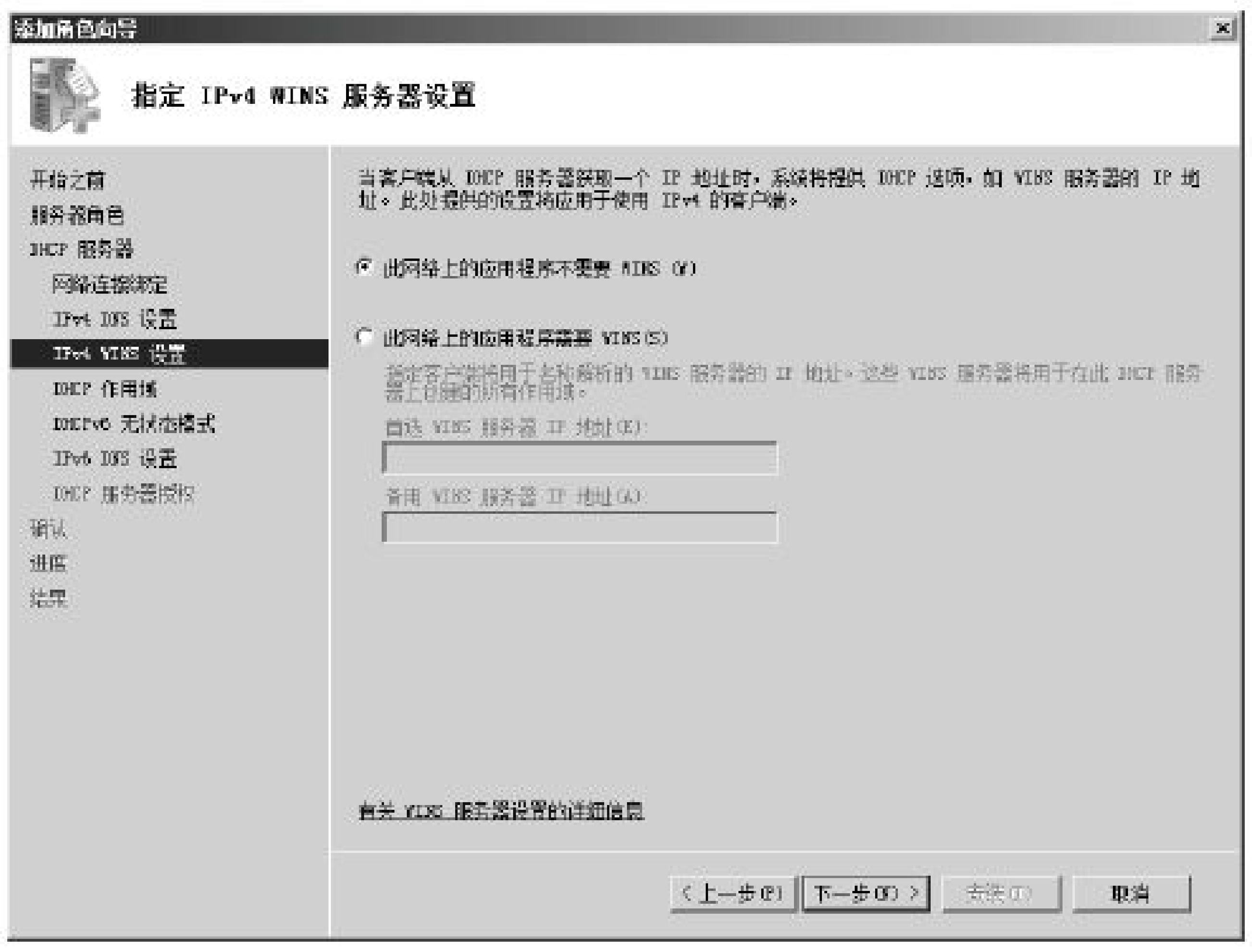


图 9-31 指定 IPv4 WINS 服务器设置(2)

图 9-32 添加或编辑 DHCP 作用域

(9) 在“添加作用域”对话框中设置作用域的名称、起始 IP 地址、结束 IP 地址、子网掩码、默认网关以及子网类型。若选中“激活此作用域”复选框，则创建完成后会自动激活，如图 9-33 所示。设置完成后，单击“确定”按钮，返回上一步操作后单击“下一步”按钮继续。

(10) 在“配置 DHCPv6 无状态模式”向导页中选择启用还是禁用服务器的 DHCPv6 无状态模式。选中“对此服务器禁用 DHCPv6 无状态模式”单选按钮，单击“下一步”按钮继续，如图 9-34 所示。

(11) 若 DHCP 服务器已加入了域，还会打开“授权 DHCP 服务器”向导页，若没有加入域，则不会出现此向导页。为 DHCP 服务器授权必须具有域管理员的权限，若当前没有以域管理员身份登录到域，则选中“使用备用凭据”单选按钮，然后单击“指定”按钮输入域管理员的用户名及密码。单击“下一步”按钮继续，如图 9-35 所示。

(12) 在“确认安装选择”向导页中，要求确认所要安装的服务器角色及配置情况，如

果配置错误，可以单击“上一步”按钮返回。单击“安装”按钮即可开始安装 DHCP 服务器角色，如图 9-36 所示。

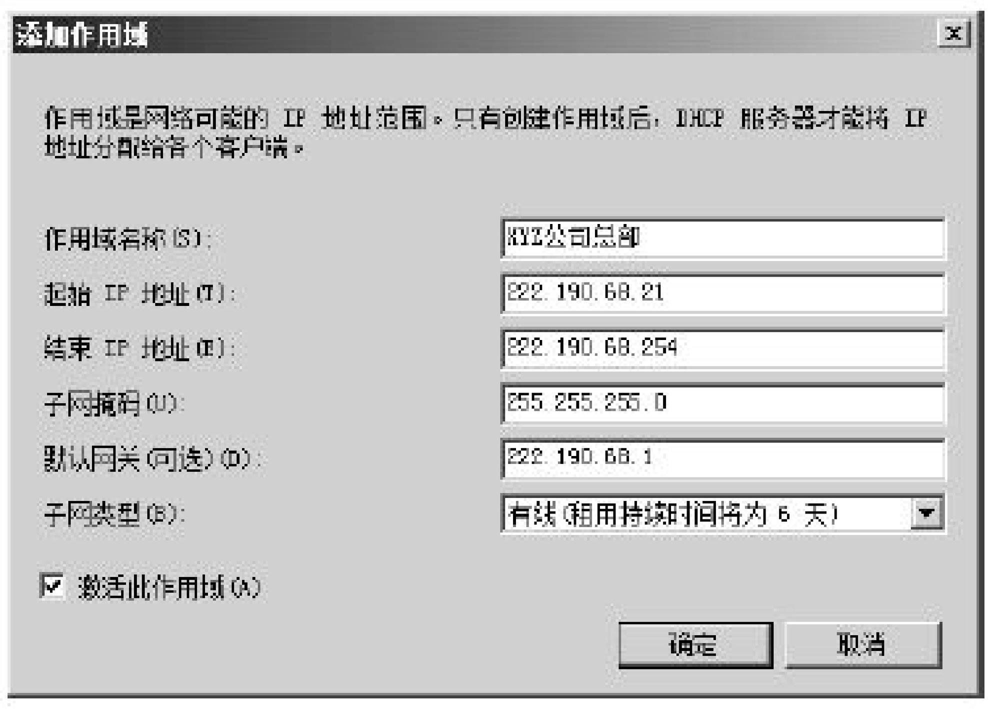


图 9-33　添加作用域

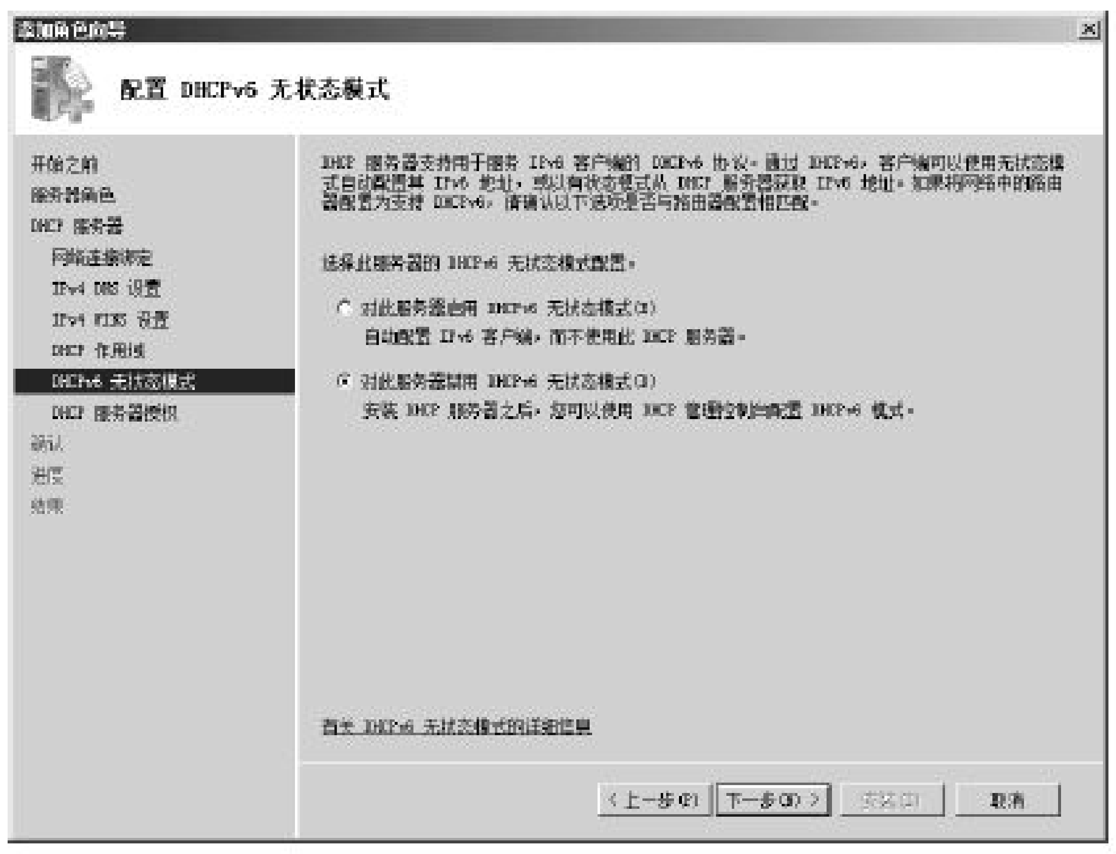


图 9-34　配置 DHCPv6 无状态模式

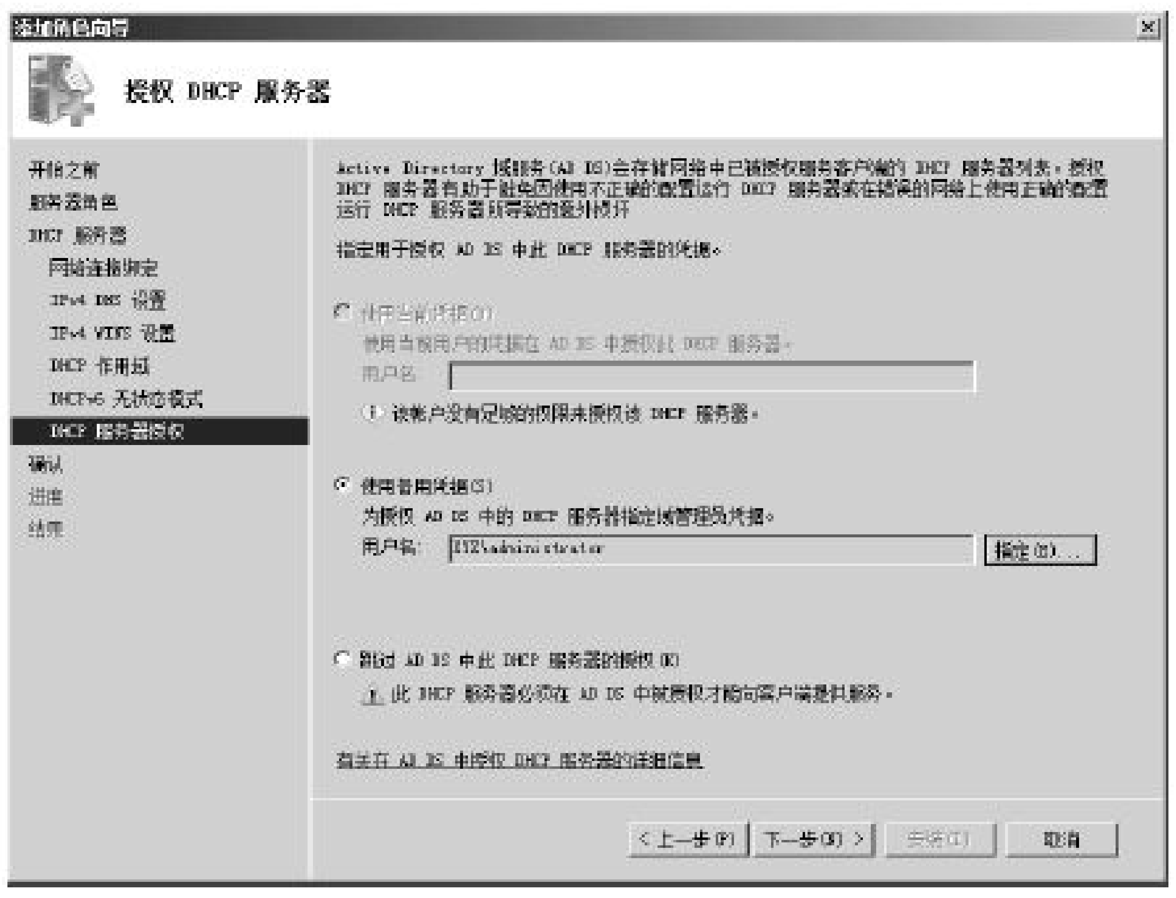


图 9-35　授权 DHCP 服务器

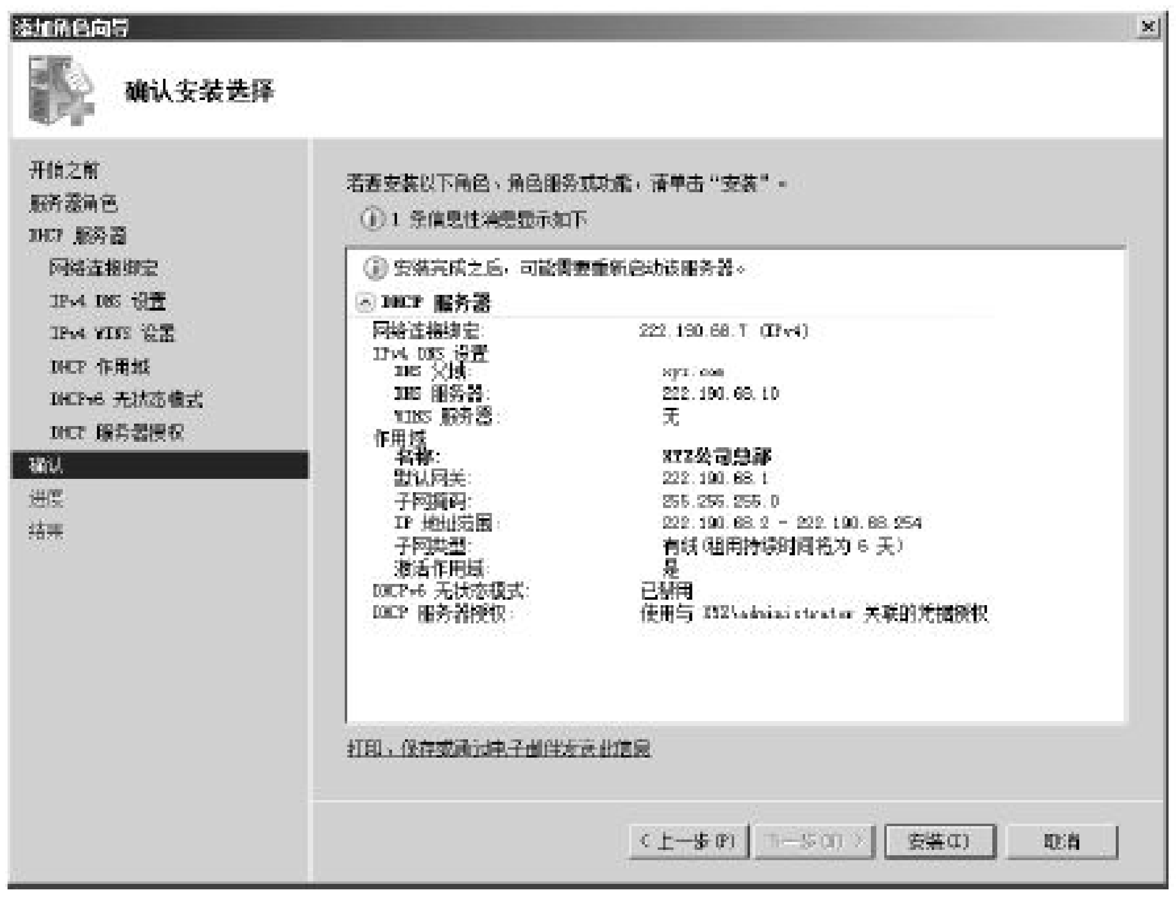


图 9-36　确认安装选择

(13) “安装进度”对话框中显示了安装 DHCP 服务器角色的进度，需耐心等待。

(14) “安装结果”对话框中显示 DHCP 服务器角色已经安装完成，提示用户可以使用 DHCP 管理器对 DHCP 服务器进行配置。若系统未启用 Windows 自动更新，还提醒用户设置 Windows 自动更新，以即时给系统打上补丁。单击“完成”按钮关闭添加角色向导，便完成了 DHCP 服务器的安装。

DHCP 服务器安装完毕后，可以通过选择“开始”→“管理工具”→DHCP 命令打开 DHCP 管理器，通过 DHCP 窗口可以管理本地或远程的 DHCP 服务器，如图 9-37 所示。

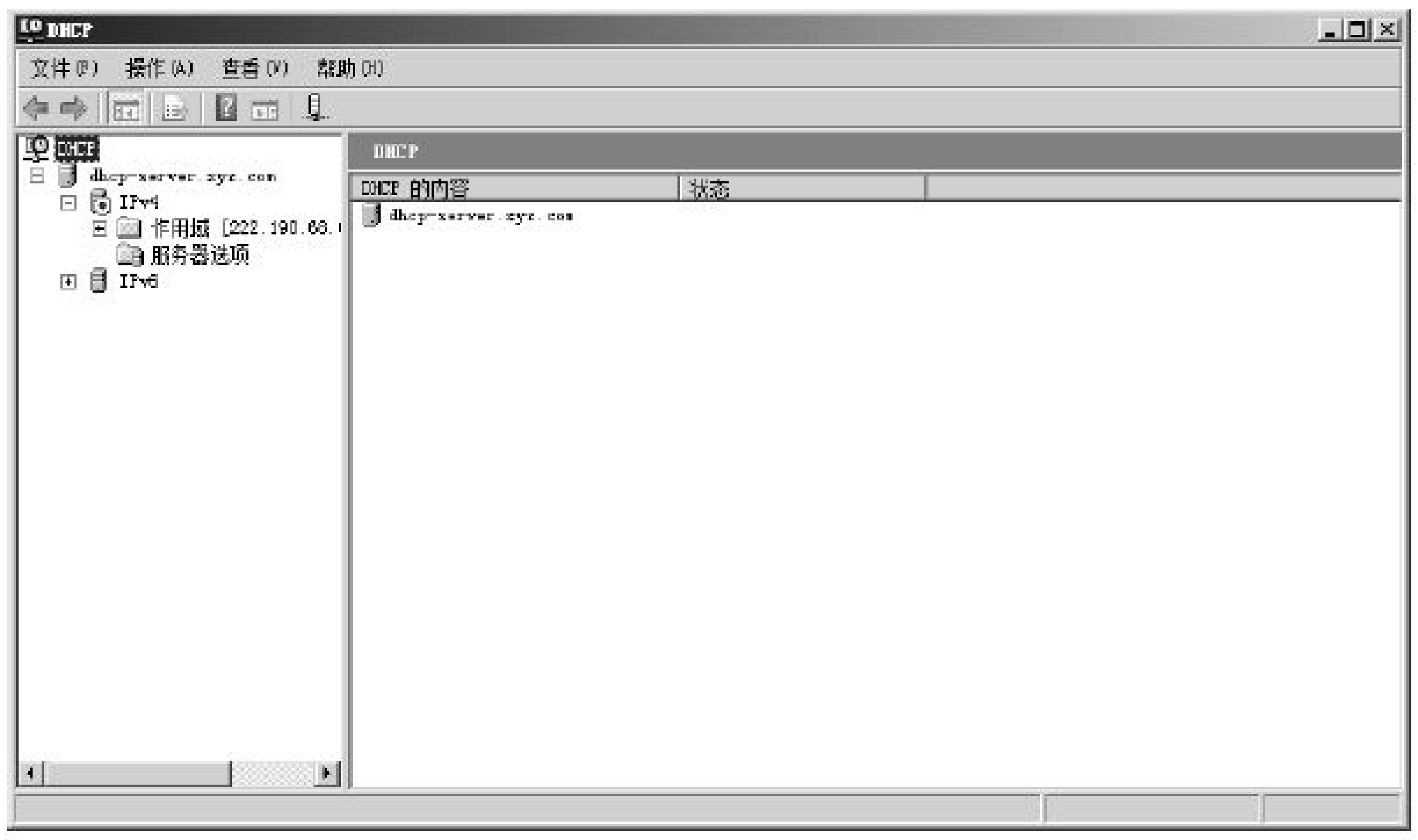


图 9-37　DHCP 管理器

2. 安装 DHCP 客户机

如果希望某台计算机能够自动获取 IP 地址，则需将这台计算机配置为 DHCP 客户机，配置方法如下。

(1) 在“控制面板”中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，选中“Internet 协议(TCP/IP)”，单击“属性”按钮，打开“Internet 协议(TCP/IP)属性”对话框。

(4) 选中“自动获得 IP 地址”单选按钮，然后单击“确定”按钮，这样便把该计算机配置为 DHCP 客户机了。

3. 设置 DHCP 服务器

在安装了 DHCP 服务器之后，还需要在 DHCP 服务器上建立一个或多个 IP 地址作用域。“IP 地址作用域”是指可以分配给 DHCP 客户机的 IP 地址范围。这样，当 DHCP 客户机向 DHCP 服务器请求 IP 地址时，DHCP 服务器就可以从 IP 地址作用域中选择一个尚未被租用的 IP 地址，将其分配给 DHCP 客户机。

新建作用域的操作步骤如下。

(1) 依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。

(2) 在左侧窗格中，右击服务器名，在弹出的快捷菜单中选择“新建作用域”命令。

(3) 在弹出的“新建作用域向导”对话框中单击“下一步”按钮。

(4) 在“名称”文本框中输入一个能够清楚表示该作用域的名称，如图 9-38 所示。

(5) 单击“下一步”按钮，打开“IP 地址范围”向导页。地址范围通过设置“起始 IP 地址”和“结束 IP 地址”来指定。通过设置“长度”，用户可以调整子网掩码，以指定 IP 地址中多少位作为网络 ID，多少位作为主机 ID，如图 9-39 所示。

图 9-38　设置作用域名

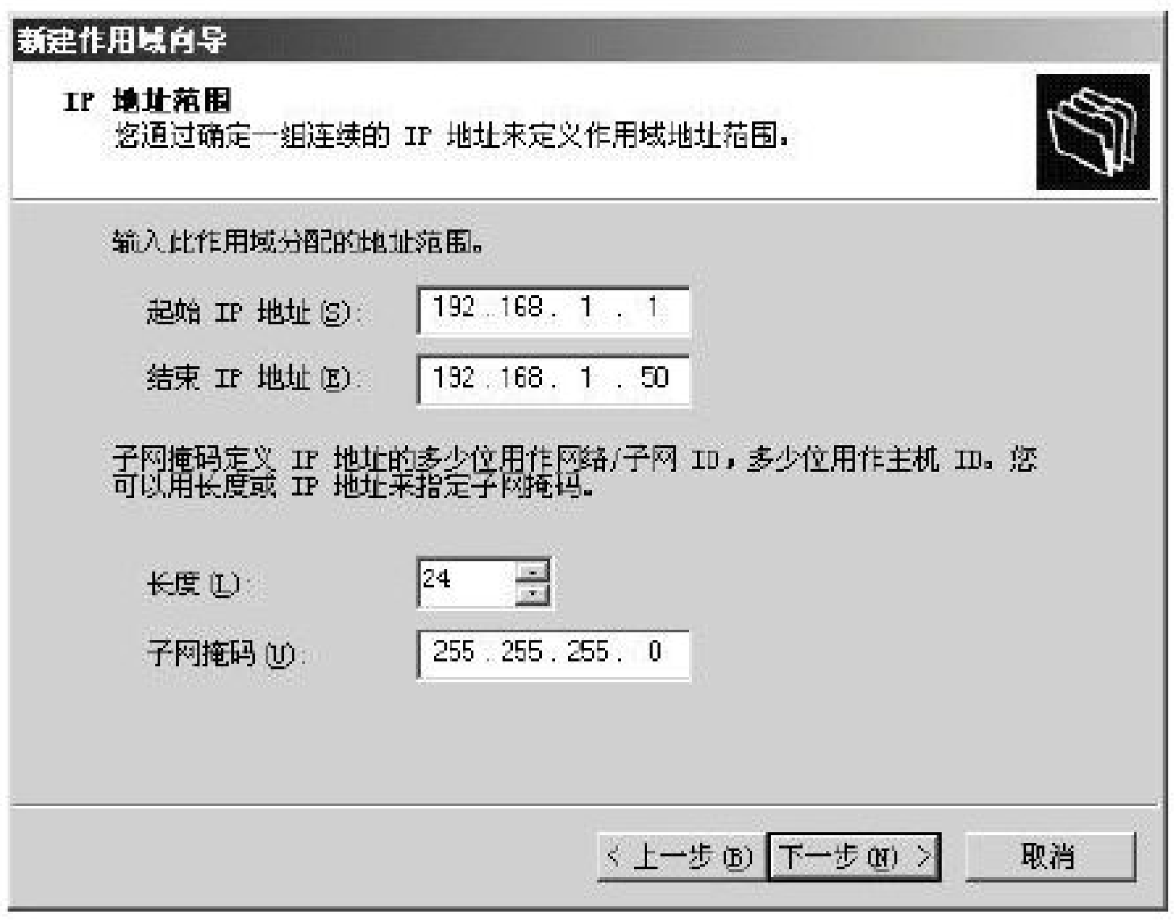


图 9-39　设置 IP 地址范围

(6) 设置好 IP 地址范围后，单击“下一步”按钮，打开“添加排除”向导页，如图 9-40 所示。这里用户可以指定前面设置的 IP 地址范围中有哪些地址不被服务器分配。如果想排除的 IP 地址是分散的，那么在“起始 IP 地址”中输入要排除的 IP 地址，然后单击“添加”按钮，重复这一过程直至所有要排除的 IP 地址均被添加。如果想排除的是某一段连续的 IP 地址，则分别输入该范围的起始 IP 地址和结束 IP 地址，然后单击“添加”按钮。

(7) 单击“下一步”按钮，打开“租约期限”向导页，如图 9-41 所示。租约期限指的是一个客户端从此作用域使用 IP 地址的时间长短。通常局域网使用的都是专用保留 IP 地址，地址数量很充裕，所以可以将租约期限设置得较长。

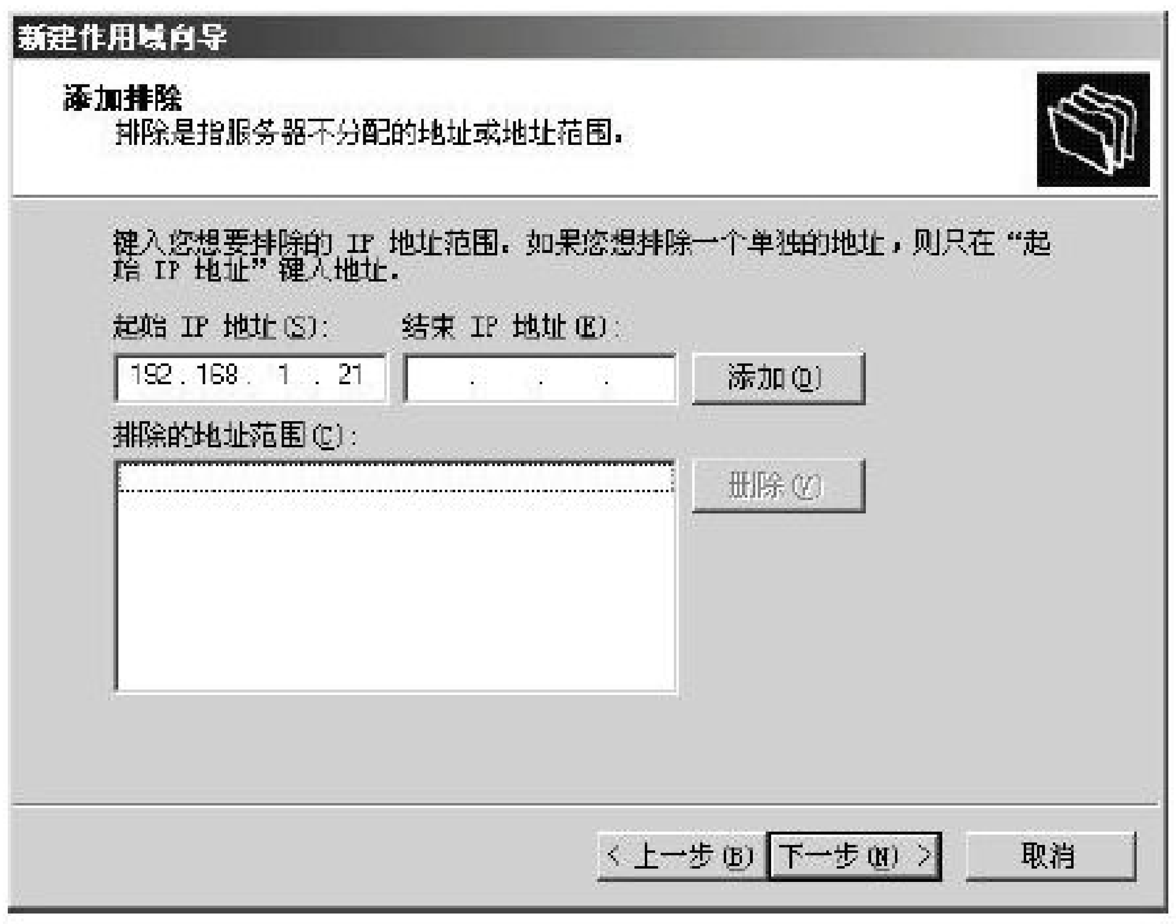


图 9-40　设置排除的 IP 地址

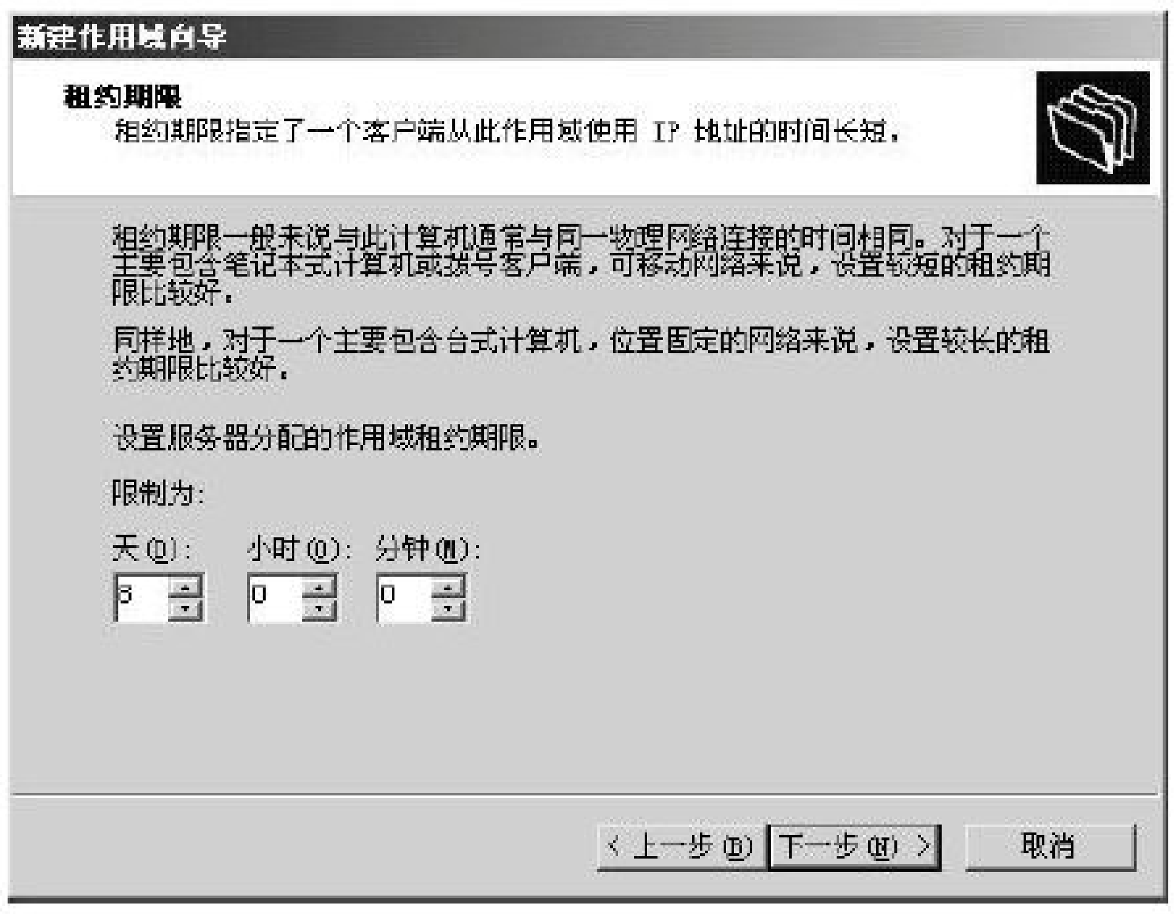


图 9-41　“租约期限”向导页

(8) 单击“下一步”按钮，向导提示用户为该作用域配置 DHCP 选项。通常只有正确配置了 DHCP 选项，DHCP 客户机才可以使用此作用域，所以选中“是，我想现在配置这些选项”单选按钮。

(9) 单击“下一步”按钮，首先要配置的是默认网关的 IP 地址。输入默认网关的 IP 地址，并单击“添加”按钮。

(10) 单击“下一步”按钮，接下来要配置的是域名称和 DNS 服务器。在“父域”文本框中输入域名，并在“IP 地址”文本框中输入 DNS 服务器的 IP 地址，然后单击“添加”按钮，如图 9-42 所示。若有多个 DNS 服务器，将其他的 DNS 服务器添加至此。通常设置两个 DNS 服务器即可，一个作为主 DNS 服务器，另一个作为辅 DNS 服务器。

(11) 单击“下一步”按钮，设置 WINS 服务器地址。如果网络中有 WINS 服务器，在“IP 地址”文本框中输入 WINS 服务器的地址，然后单击“添加”按钮，如图 9-43 所示。

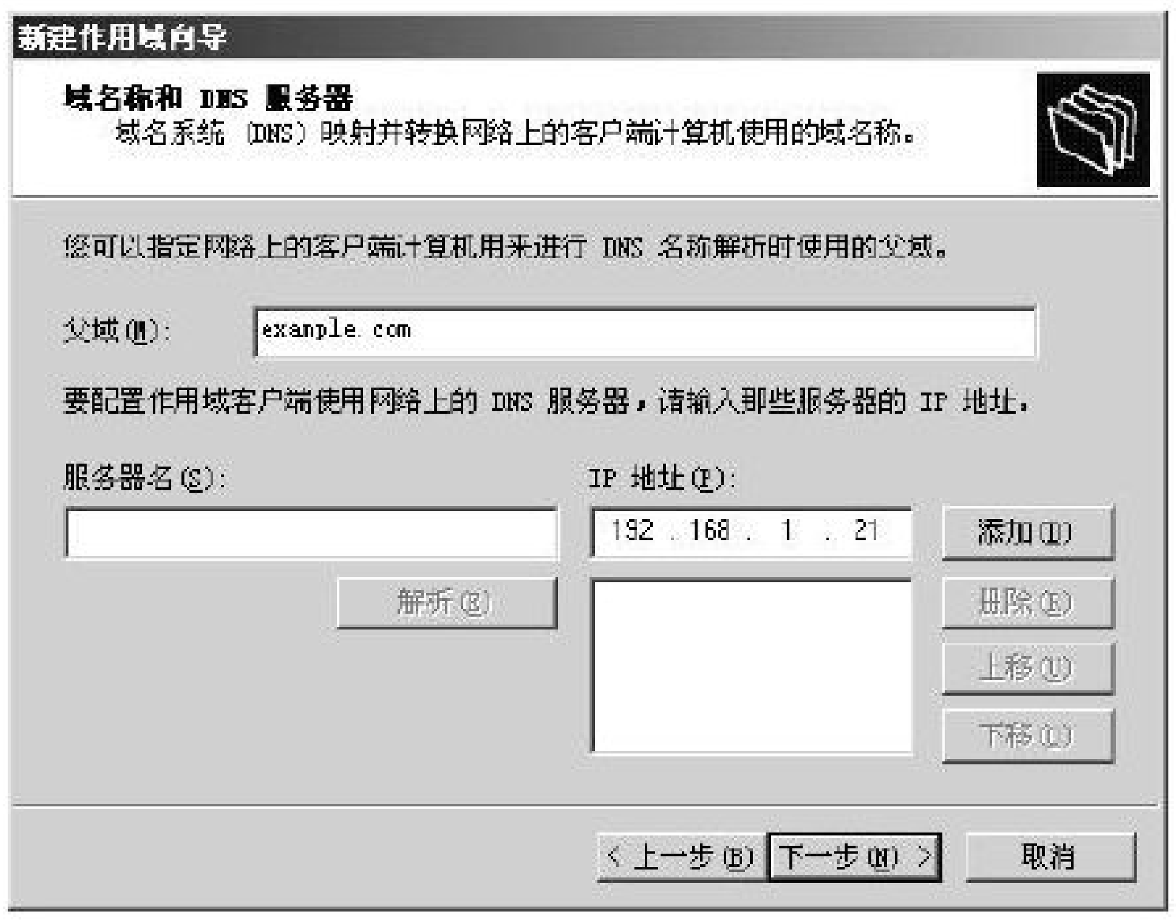


图 9-42　设置域名和 DNS 服务器

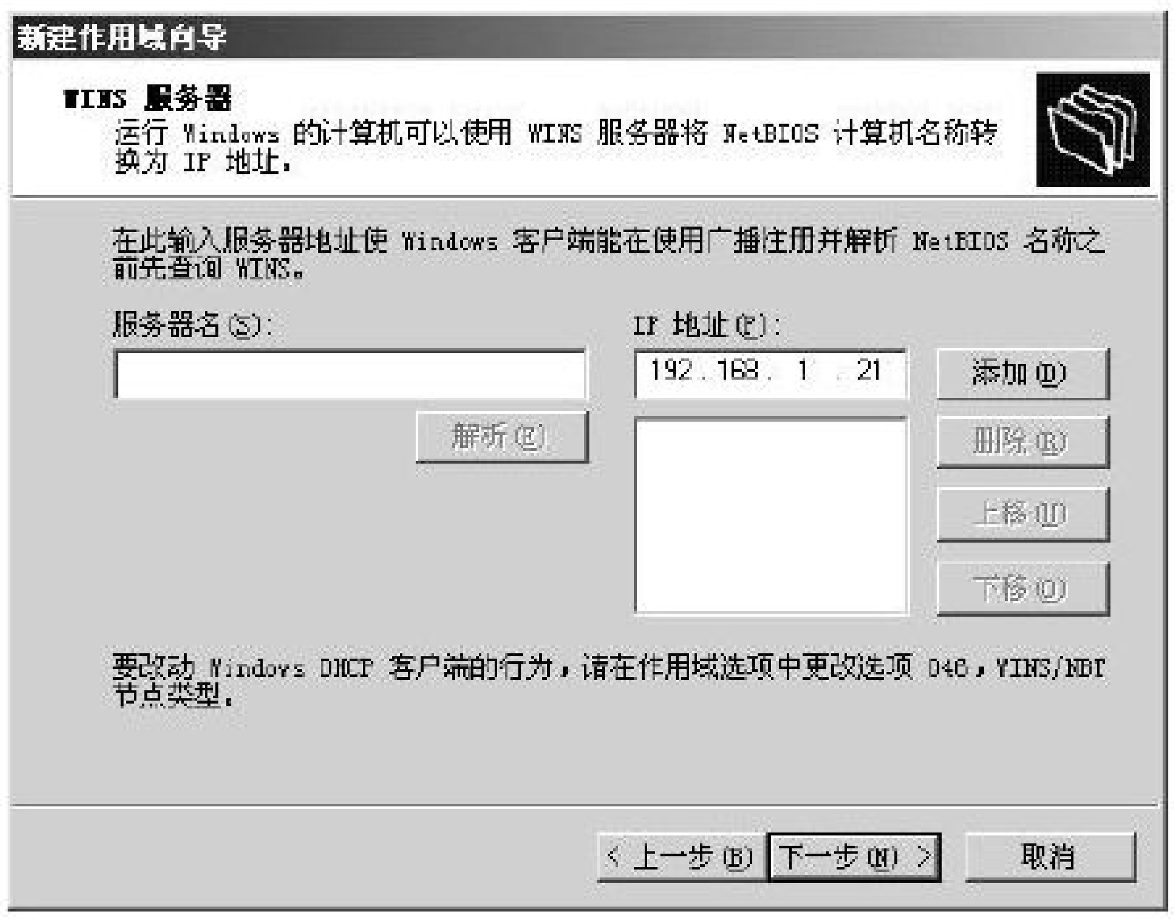


图 9-43　设置 WINS 服务器

(12) 单击“下一步”按钮，向导会提示是否激活此作用域，选择“是，我想现在激活此作用域”。

(13) 单击“下一步”按钮，向导提示已成功完成了新建作用域，单击“完成”按钮关闭向导。

接下来，系统会创建新的作用域。创建完成后的控制台如图 9-44 所示。展开新建的作用域，选择“地址池”选项，可以查看当前地址池中 IP 地址的范围及被排除的 IP 地址。选择“地址租约”选项，可以查看当前有哪些客户端租用了哪些 IP 地址。选择“保留”选项，可以查看并设置将地址池中的某些 IP 地址永久地分配给一些客户端。新建保留地址的方法是右键单击“保留”选项，在弹出的快捷菜单中选择“新建保留”命令，然后在弹出的对话框中输入相应的信息即可。需要注意的是，设置保留地址时，需要知道客户端网卡的 MAC 地址，即物理地址。网卡的物理地址可通过在“命令提示符”中运行 ipconfig /all 命令查看。

选择“作用域选项”选项，可以查看当前为该作用域设置的选项，也就是前面新建作用域向导中所设置的路由器、域名、DNS 服务器和 WINS 服务器等信息。这些是保证客户端能正常访问网络所必需的信息。如果用户还需要为该作用域设置其他的附加选项，可右击“作用域选项”，在弹出的快捷菜单中选择“配置选项”命令，如图 9-45 所示。打开如图 9-46 所示的“作用域 选项”对话框，在“可用选项”中选中要设置的选项，并在下面设置相应的信息，然后单击“确定”按钮即可。

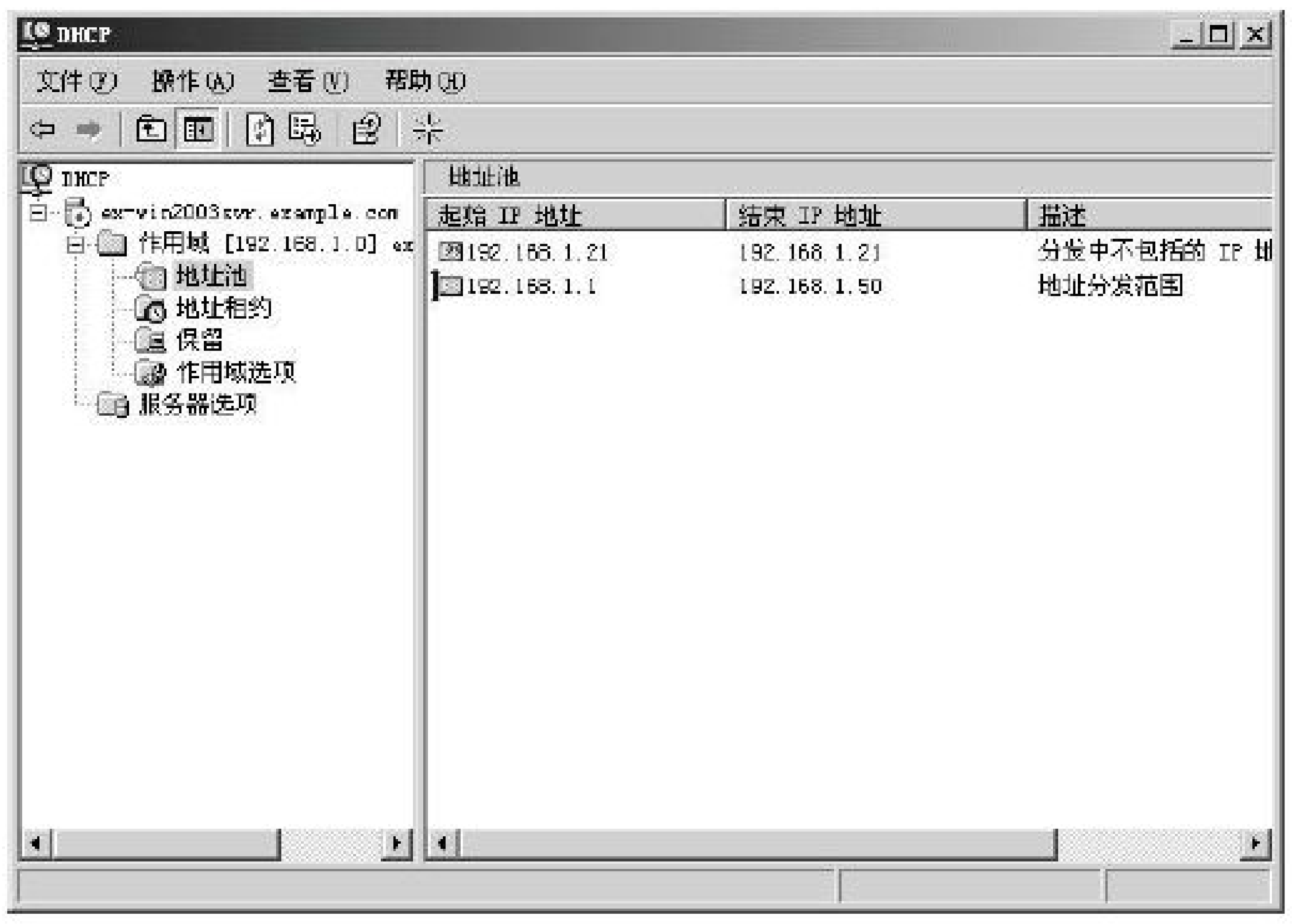


图 9-44　DHCP 服务器的地址池

图 9-45　选择“配置选项”命令

右击新建的作用域，在弹出的快捷菜单中选择“属性”命令，可以对作用域的设置进行更改。作用域的属性对话框共有 3 个选项卡：“常规”、DNS 和“高级”选项卡。

“常规”选项卡如图 9-47 所示，在此可以更改作用域名、IP 地址范围和租约期限。

图 9-46　“作用域 选项”对话框

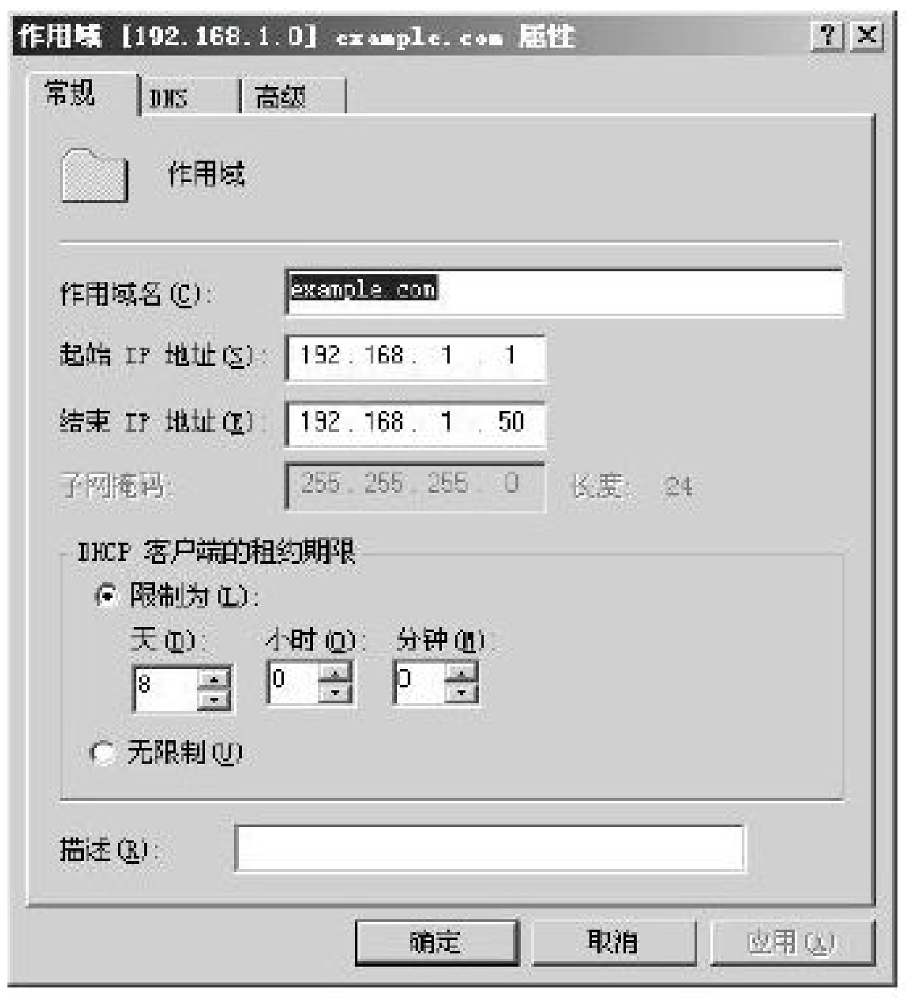


图 9-47　“常规”选项卡

DNS 选项卡可以设置 DHCP 服务器是否启用 DNS 动态更新。启用 DNS 动态更新的好

处是当客户端的 IP 地址发生变化后，DHCP 服务器将会发送信息更新 DNS 服务器中该主机的主机和指针记录，以确保信息的一致性。

“高级”选项卡可以指定 DHCP 服务器为哪种类型的客户端动态分配 IP 地址，其中 BOOTP 一般为无盘工作站客户端，若网内没有无盘工作站，选择“仅 DHCP”选项即可。

当安装 DHCP 服务器的计算机同时也是域控制器时，在使用 DHCP 服务器前需对其进行授权，这是因为当错误配置或未授权的 DHCP 服务器被引入网络时，可能会引发问题。例如，如果启动了未授权的 DHCP 服务器，它可能会为客户端租用不正确的 IP 地址或者否认尝试续订当前地址租约的 DHCP 客户端。这两种配置中的任何一个都可能导致启用 DHCP 的客户端产生更多的问题。例如，从未授权的服务器获取配置租约的客户端将找不到有效的域控制器，从而导致客户端无法成功登录到网络。为了避免这些问题，在客户端之前运行 Windows Server 2008 R2 上的 DHCP 服务器服务时，需要验证是否已在 Active Directory 中对它们进行了授权。这样就避免了由于运行带有不正确配置的 DHCP 服务器或者在错误的网络上运行配置正确的服务器而导致的大多数意外破坏。DHCP 服务器一旦在授权列表中发现其 IP 地址，便进行初始化并开始为客户端提供 DHCP 服务。如果在授权列表中未发现自己的地址，则不进行初始化并停止提供 DHCP 服务。

授权的某台 DHCP 服务器的操作方法如下：依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。右击要授权的服务器名，在弹出的快捷菜单中选择“授权”命令。授权过程需要一段时间，期间用户可以按 F5 键查看状态，检查是否完成授权。

要解除某台已授权服务器的授权，方法与授权过程相同，只是在弹出的快捷菜单中选择“撤销授权”命令即可。

9.6.1.3　Linux DHCP 服务器的配置

DHCP 的配置文件是/etc/dhcpd.conf，不过默认的情况下这个文件不存在，需要使用它的模板建立一个配置文件。模板的位置在/usr/share/doc/dhcp-3.0p11/dhcpd.conf.sample 中。

模板配置文件内容如下：

```
ddns-update-style interim;
#配置使用过渡性 DHCP-DNS 互动更新模式
ignore client-updates;
#忽略客户端更新
subnet 192.168.0.0 netmask 255.255.255.0 {
#设置子网声明
# --- default gateway
option routers 192.168.0.1;
#设置默认网关为 192.168.0.1

option subnet-mask 255.255.255.0;
#设置客户端的子网掩码
option nis-domain "domain.org";
#为客户设置 NIS 域
option domain-name "domain.org";
#为客户设置域名
option domain-name-servers 192.168.1.1;
```

```
#为客户设置域名服务器
option time-offset -18000; # Eastern Standard Time
#设置偏移时间
option ntp-servers 192.168.1.1;
#设置 NTP 服务器
option netbios-name-servers 192.168.1.1;
#设置 WINS 服务器
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
# option netbios-node-type 2;
#设置 netbios 节点类型
range dynamic-bootp 192.168.0.128 192.168.0.255;
#设置动态的地址池
default-lease-time 21600;
#设置默认的地址租期

max-lease-time 43200;
#设置客户端最长的地址租期

# we want the nameserver to appear at a fixed address
//设置主机声明
host ns {
next-server marvin.redhat.com;
//设置定义服务器从引导文件中装入的主机名，用于无盘站
hardware ethernet 12:34:56:78:AB:CD;
//指定 DHCP 客户的 MAC 地址
fixed-address 209.175.42.254;
//给指定的 MAC 地址分配 IP
}
}
```

9.6.2 典型例题分析

例 9-19 在 Windows 环境下，租约期满后，DHCP 客户端可以向 DHCP 服务器发送一个__(36)__报文来请求重新租用 IP 地址。(2017 年下半年真题 36)

A. dhcpdiscover B. dhcprequest C. dhcprenew D. dhcpsack

解析： DHCP 典型报文中没有 dhcprenew，重新申请 IP 地址还是使用 dhcpdiscover 来实现。

答案： A

例 9-20 在某台 PC 上运行 ipconfig /all 命令后得到如下结果，下列说法中正确的是__(43)__。(2017 年下半年真题 43)

```
Windows IP Configuration
Host Name . . . . . . . . . . . . . . :MSZFA2SWBGXX4UT
primaly Dns Suffix……:
Node Type . . . . . . . . . . . . . . :Hybrid
```

```
IP Routing Enabled. . . . . . . . . :No
WINS Proxy Enabled……: No
DNS Suffix Search List. ……: home
Wireless LAN adapter:
Connection-specific DNS Suffix.:home
Description . . . . . . . . . . . . :Realtek RTL8188EU Network Adapter
Physical Address. . . . . . . .. . . . : 30-B4-9E-12-F2-ED
DHCP Enabled…… …: Yes
Autoconfiguration Enabled . . . :Yes
Link -local IPv6 Address . .. . :fe80::40bl:7a3a:6cd2:1193%12(peferred)
IPv4Address. . . . . . . .…. . . .: 192.168.3.12(preferred)
Subnet mask . . . . . . . .. . . : 255.255.255.0
Lease Obtained. . . . . " . . . :2017-7-15 20:01:59
Lease Expires .. . . . . . . . . .: 2017-7-16 20:01:59
Default Gateway . . . . . . " . : 192.168.3.1
DHCP.Server……: 10.10.20.3
DHCPv6IAID…… ……: 222857938
DHCPv6Client DU1D……: 00-01-00-01-1F-88-22-5F-74-DO-2B-7B-88-29
DNS Servers . . . . . . . . . . . : 8.8.8.8
192.168.3.1
NetBIOS over Tepip . . . . . . . : Enabled
```

A. IP 地址 192.168.3.12 是该 PC 未续约过的 IP 地址

B. 该 PC 的 IP 地址租期为 12 个小时

C. 该 PC 与 DHCP 服务器位于同一个网段

D. 进行 DNS 查询时首先查询服务器 8.8.8.8

解析：DHCP 服务器默认首选分配客户机曾经使用过的 IP 地址，且租约由 15 号到 16 号为 24 小时，DHCP 服务器指定为客户分配的 DNS 服务器地址第一个为 8.8.8.8。

答案：D

例 9-21　当 DHCP 服务器拒绝客户端的 IP 地址请求时发送__(33)__报文。(2016 年下半年真题 33)

A. DhcpOffer　　B. DhcpDecline　　C. DhcpAck　　D. DhcpNack

解析：DhcpNack 报文是服务器无法正常分配 IP 时发送给客户端的报文，当 DHCP 服务器拒绝客户端的 IP 地址请求时发送 DhcpNack 报文。DhcpOffer 报文是服务器预提供 IP 的报文。DhcpDecline 报文是客户端发送给服务器的报文，通知所分配的 IP 地址不可用。DhcpAck 报文是服务器发给客户端的报文，带有分配的 IP 的租期。此外，DhcpDiscover 报文是客户端发送给服务器请求 IP 租用的报文。DhcpRequest 报文是客户端确认使用 IP 发送给服务器的报文。 DhcpRelease 报文是用于客户端释放 IP 地址发送给服务器的。

答案：D

例 9-22　下面是 DHCP 协议工作的 4 种消息，正确的顺序应该是__(40)__。(2016 年下半年真题 40)

①DHCP　Discovery

②DHCP　Offer

③DHCP　Request

④DHCP　Ack

A. ①③②④　　B.①②③④　　C.②①③④　　D.②③①④

解析：DHCP 协议采用 UDP 作为传输协议，主机发送请求到 DHCP 服务器的 67 号端口，DHCP 服务器回应应答消息给主机的 68 号端口。

DHCP Client 以广播的方式发出 DHCP Discover 报文。

所有的 DHCP Server 都能够接收到 DHCP Client 发送的 DHCP Discover 报文，所有的 DHCP Server 都会给出响应，向 DHCP Client 发送一个 DHCP Offer 报文。

DHCP Client 只能处理其中的一个 DHCP Offer 报文，一般的原则是 DHCP Client 处理最先收到的 DHCP Offer 报文。

DHCP Client 会发出一个广播的 DHCP Request 报文，在选项字段中会加入选中的 DHCP Server 的 IP 地址和需要的 IP 地址。

DHCP Server 收到 DHCP Request 报文后，判断选项字段中的 IP 地址是否与自己的地址相同。如果不相同，DHCP Server 不做任何处理，只清除相应 IP 地址分配记录；如果相同，DHCP Server 就会向 DHCP Client 响应一个 DHCP Ack 报文，并在选项字段中增加 IP 地址的使用租期信息。

DHCP Client 接收到 DHCP Ack 报文后，检查 DHCP Server 分配的 IP 地址是否能够使用。如果可以使用，则 DHCP Client 成功获得 IP 地址并根据 IP 地址使用租期自动启动续延过程；如果 DHCP Client 发现分配的 IP 地址已经被使用，则 DHCP Client 向 DHCP Server 发出 DHCP Decline 报文，通知 DHCP Server 禁用这个 IP 地址，然后 DHCP Client 开始新的地址申请过程。

DHCP Client 在成功获取 IP 地址后，随时可以通过发送 DHCP Release 报文释放自己的 IP 地址，DHCP Server 收到 DHCP Release 报文后，会回收相应的 IP 地址并重新分配。

答案：B

9.6.3 同步练习

1. 以下关于 DHCP 协议的描述中，错误的是_____。
   A. DHCP 客户机可以从外网段获取 IP 地址
   B. DHCP 客户机只能收到一个 dhcpoffer
   C. DHCP 不会同时租借相同的 IP 地址给两台主机
   D. DHCP 分配的 IP 地址默认租约期为 8 天
2. DHCP 客户端不能从 DHCP 服务器获得_____。
   A. DHCP 服务器的 IP 地址　　B. Web 服务器的 IP 地址
   C. DNS 服务器的 IP 地址　　D. 默认网关的 IP 地址
3. Linux 系统中，默认安装 DHCP 服务的配置文件为_____。
   A. /etc/dhcpd.conf　　B. /etc/dhcp.conf
   C. /etc/dhcpd.config　　D. /etc/dhcp.config
4. 某 Linux DHCP 服务器 dhcpd.conf 的配置文件如下：

```
ddns-update-style none;
```

```
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.200 192.168.0.254;
  ignore client-updates;
  default-lease-time 3600;
  max-lease-time 7200;
  option routers 192.168.0.1;
  option domain-name "test.org";
  option domain-name-servers 192.168.0.2;
}
host test1 {hardware ethernet 00:E0:4C:70:33:65; fixed-address 192.168.0.8;}
```

客户端 IP 地址的默认租用期为________小时。

A. 1　　B. 2　　C. 60　　D. 120

5. 可以把所有使用 DHCP 协议获取 IP 地址的主机划分为不同的类别进行管理。下面的选项列出了划分类别的原则，其中合理的是_____。

A. 移动用户划分到租约期较长的类　　B. 固定用户划分到租约期较短的类

C. 远程访问用户划分到默认路由类　　D. 服务器划分到租约期最短的类

6. 在 Windows 环境下，DHCP 客户端可以使用__(1)__命令重新获得 IP 地址，这时客户机向 DHCP 服务器发送一个__(2)__数据包来请求租用 IP 地址。

(1) A. ipconfig/release　　B. ipconfig/reload

C. ipconfig/renew　　D. ipconfig/all

(2) A. Dhcpoffer　　B. Dhcpack

C. Dhcpdiscover　　D. Dhcprequest

7. 为保证在启动 Linux 服务器时自动启动 DHCP 进程，应在______文件中将配置项 dhcpd=no 改为 dhcpd=yes。

A. /etc/rc.d/rc.inet1　　B. /etc/rc.d/rc.inet2

C. /etc/dhcpd.conf　　D. /etc/rc.d/rc.s

9.6.4　同步练习参考答案

1. B　　2. B　　3. A　　4. A　　5. C　　6. (1) C　　(2) C　　7. A

9.7　Samba 服务器的配置

9.7.1　考点辅导

1. Samba 协议基础

20 世纪 80 年代早期由 IBM 和 Sytec 合作开发了一套用于网络通信接口调用的 NetBIOS 协议。在 NetBIOS 出现之后，为了使 Windows 主机间的资源能够共享，Microsoft 实现了一个基于 NetBIOS 协议的共享网络文件/打印服务系统，Microsoft 称为 SMB(Server Message Block，服务信息块)通信协议，通过 SMB 协议，使网络上不同计算机之间能够共

享打印机、文件和串口通信等服务。

随着网络应用技术的发展和 Internet 的流行，Microsoft 为了使 SMB 协议得到更广泛的应用，就将 SMB 协议进行整理，重新命名为 CIFS(Common Internet File System)，使其成为网络和 Internet 上计算机之间相互共享数据的一个标准协议。它可以为网络内部的其他 Windows 和 Linux 机器提供文件系统、打印服务或其他一些信息服务。SMB 的工作原理是让 NetBIOS 与 SMB 这两种协议运行在 TCP/IP 的通信协议上，且通过 NetBIOS nameserver 使用户的 Linux 机器可以在 Windows 的网络邻居上被看到。所以就可以和 Windows 的机器在网络上相互沟通，共享文件与服务了。

SMB 协议是一种客户机/服务器协议，SMB 客户机使用 TCP/IP、NetBEUI 或 IPX/SPX 与服务器连接，当使用 TCP/IP 时，实际上使用的是在 TCP/IP 上的 NetBIOS。因此基于 SMB 的网络使用的底层协议虽然不一样，但其核心还是让基于 NetBEUI 的 NetBIOS 和基于 TCP/IP 的 NetBIOS 这两种协议都运行在 TCP/IP 的通信协议上，并通过 NetBIOS nameserver 使网络中 Linux 系统用户的机器可以在 Windows 的网络邻居上被看到，从而就可以和 Windows 的机器在网络上相互沟通、共享文件与服务了。目前，类似这种资源共享的通信协议还有 NFS、Appletalk、NetWare 等。

2. Samba 主要功能

具体说来，Samba 主要有以下功能。

(1) Samba 服务器向 Linux 或 Windows 系统客户端提供 Windows 风格的文件和打印机共享服务，实现安装在 Samba 服务器上的打印机和文件系统的共享。

(2) 支持 WINS 名字服务器的解析及浏览。在 Windows 网络中，为了能够利用网上资源，同时自己的资源也能被别人所利用，各个主机都定期地向网上广播自己的身份信息。而负责收集这些信息，为别的主机提供检索情报的服务器就被称为浏览服务器。Samba 可以有效地完成这项功能，在跨越网关的时候，Samba 还可以作为 WINS 服务器使用。

(3) 提供 SMB 客户功能，利用 Samba 提供的 SMB 客户机程序可以从 Linux 下以类似于 FTP 的方式访问 Windows 的资源。

(4) 备份 PC 上的资源，利用一个叫 Smbtar 的 Shell 脚本，可以使用 tar 格式备份和恢复一台远程 Windows 上的共享文件。

(5) 支持 Windows 域控制器和 Windows 成员服务器对使用 Samba 资源的用户进行认证。提供一个命令行工具，可以有限制地支持 Windows 的某些管理功能。

(6) 支持 SSL(安全套接层)协议。

3. Samba 的简单配置

Samba 能够使 Windows 用户通过“网上邻居”等熟悉的方式直接访问 Linux 上的资源，也能使 Linux 利用 SMB 客户端程序访问 Windows 的共享资源。

下面以一个具体的例子对 Samba 服务器的配置进行说明。

```
[global]
   workgroup = WORKGROUP
   server string = Samba Server
   printcap name = /etc/printcap
   load printers = yes
```

```
cups options = raw
log file = /var/log/samba/%m.log
   max log size = 50
   security = user
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   dns proxy = no
   idmap uid = 16777216-33554431
   idmap gid = 16777216-33554431
   template shell = /bin/false
   winbind use default domain = no
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
[printers]
   comment = All Printers
   path = /var/spool/samba
   browseable = no
   guest ok = no
   writable = no
   printable = yes
```

从上面的程序中可以看到 Samba 的配置文件分为 3 节。

[global]：这个小节主要包含全局参数。

[homes]：这个小节用于共享存储在\home 中的 Linux 用户目录。

[printers]：这个小节用于共享本地 Linux 打印机文件/etc/printcap 中列出的所有打印机。

9.7.2　典型例题分析

例 9-23　__(33)__是 Linux 中 Samba 的功能。(2017 年下半年真题 33)

A. 提供文件和打印机共享服务　　B. 提供 FTP 服务

C. 提供用户的认证服务　　D. 提供 IP 地址分配服务

解析：Samba 在 Linux 中是一项提供文件和打印共享的基本服务。

答案：A

例 9-24　Linux 系统中，______服务的作用与 Windows 的共享文件服务作用相似，提供基于网络的共享文件/打印服务。

A. Samba　　B.Ftp　　C. SMTP　　D. Telnet

解析：为了使 Windows 主机间的资源能够共享，Microsoft 实现了一个基于 NetBIOS 协议的共享网络文件/打印机系统，Microsoft 称为 SMB 通信协议。Samba 就是用来实现 SMB 的一种软件。Samba 服务器向 Linux 或 Windows 系统客户端提供 Windows 风格的文件和打印机共享服务，实现在 Samba 服务器上的打印机和文件系统的共享。

答案：A

9.7.3 同步练习

关于 Samba 的功能，下列说法错误的是________。

A. 支持 WINS 名字服务器的解析及浏览

B. 不支持 SSL(安全套接层)协议

C. 提供 Windows 风格的文件和打印机共享服务

D. 可以使用 tar 格式备份和恢复一台远程 Windows 上的共享文件

9.7.4 同步练习参考答案

B

9.8 Windows Server 2008 R2 的安全策略

9.8.1 考点辅导

Windows Server 2008 R2 的安全策略定义了用户在使用计算机、运行应用程序和访问网络等方面的行为，通过这些约束避免对网络安全性的有意或无意的伤害。

安全策略是一个事先定义好的一系列应用计算机的行为准则，应用这些安全策略保证用户有一致的工作方式，防止用户破坏计算机上的各种重要的配置，并保护网络上的敏感数据。

在 Windows Server 2008 R2 中安全策略分为“本地安全策略”和“组策略”两种。本地安全策略实现基于单个计算机的安全性对于较小的企业或组织，或者是在网络中没有应用活动目录的网络，通常使用本地安全策略；而组策略可以在站点、组织单元(OU)或域的范围内实现，通常应用于较大规模并且实施活动目录的网络中。

9.8.2 典型例题分析

例 9-25 下列说法错误的是________。

A. 安全策略是一个事后定义的行为准则

B. 应用安全策略保证用户有一致的工作方式

C. 安全策略防止用户破坏计算机上的各种重要的配置

D. 安全策略保护网络上的敏感数据

解析：安全策略是事先定义好的一系列应用计算机的行为准则。

答案：A

9.8.3　同步练习

下列说法错误的是________。

A. 本地安全策略适用于较小的企业或组织

B. 在网络中没有应用活动目录的网络通常使用本地安全策略

C. 组策略可以在站点、组织单元(OU)或域的范围内实现

D. 本地安全策略应用于较大规模并且实施活动目录的网络中

9.8.4　同步练习参考答案

D

9.9　本 章 小 结

本章知识点在 2014 年的新大纲中改动不大，主要是知识点的明确化、具体化。

本章要求考生掌握网络操作系统的相关知识，包括网络操作系统的功能、分类和特点、Windows 2008 R2 平台下的系统管理和网络应用、DHCP 服务器的原理和配置、网络系统管理、DNS、电子邮件服务器配置、WWW 及 FTP 服务器。

本章相关知识点在历次考试中分布相对集中，分值在 9 分左右，是考试的重点。根据往年的考题，网络操作系统的重点是 Windows Server 2008 R2 和 Linux 下的网络配置、网络诊断以及常用的网络应用服务(如 DHCP 服务、DNS 服务、WWW 服务等)。网络操作系统的知识繁多，对网络操作系统的学习关键要掌握大纲的精神，明确考试范围，以常考的典型例题为主线，抓住重点。本章的前几节都组织了针对水平考试的典型例题分析和同步训练，这些题目涵盖了大纲规定的知识要点。

9.10　达标训练题及参考答案

9.10.1　达标训练题

1. 有多种方案可以在一台服务器中安装 Windows 和 Linux 两种网络操作系统，其中可以同时运行 Windows 和 Linux 两种网络操作系统的方案是________。

A. GRUB 多引导程序　　B. LILO 多引导程序

C. VMWare 虚拟机　　D. Windows 多引导程序

2. Linux 系统中的文件操作命令 grep 用于________。

A. 列出文件的属性信息　　B. 在指定路径查找文件

C. 复制文件　　D. 在指定文件中查找指定的字符串

3. 在某台主机上无法访问域名为 aaa.bbb.cn 的网站，而局域网中的其他主机可正常访

问，在该主机上执行 ping 命令时有如下的信息：

```
C:\>ping aaaa.bbbb.cn
Ping ping aaaa.bbbb.cn[202.112.0.36] with 32 bytes of data:
Reply from 202.112.0.36: Destination net unreachable
Reply from 202.112.0.36: Destination net unreachable
Reply from 202.112.0.36: Destination net unreachable
Reply from 202.112.0.36: Destination net unreachable

Ping statistics for 202.112.0.36:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% lost)
Approximate round trip times in milli-seconds:
   Minimum = 0ms，Maximum = 0ms，Average = 0ms
```

分析以上信息，可能造成该现象的原因是________。

A. 该计算机设置的 DNS 服务器工作不正常

B. 该计算机设置的 TCP/IP 工作不正常

C. 该计算机连接的网络中的相关网络设备配置了拦截的 ACL 规则

D. 该计算机网关地址设置错误

4. 在 Windows Server 2003 中，创建用户组时，可选择的组类型中，仅用于分发电子邮件且没有启用安全性的是________。

A. 安全组　　B. 本地组　　C. 全局组　　D. 通信组

5. 在 Windows Sever 2003 中，与 Windows 2000 Sever 终端服务对应的是________。

A. 远程协助　　B. 管理远程桌面

C. 远程管理的 Web 界面　　D. 远程安装服务

6. 在接收邮件时，客户端代理软件与 POP3 服务器通过建立________连接来传送报文。

A. UDP　　B. TCP　　C. P2P　　D. DHCP

7. 在 Windows Server 2003 操作系统中，WWW 服务包含在______组件下。

A. DNS　　B. DHCP　　C. FTP　　D. IIS

8. 在下列选项中，属于 IIS 6.0 提供的服务组件的是______。

A. Samba　　B. FTP　　C. DHCP　　D. DNS

9. 在 Windows 系统中，默认权限最低的用户组是______。

A. everyone　　B. administrators　　C. power users　　D. users

10. 下面的 Linux 命令中，能关闭系统的命令是______。

A. kill　　B. shutdown　　C. exit　　D. logout

11. 在 Linux 中，可以利用______命令来终止某个进程。

A. kill　　B. dead　　C.quit　　D. exit

12. DNS 服务器中提供了多种资源记录，其中______定义了区域的授权服务器。

A. SOA　　B. NS　　C. PTR　　D. MX

13. DNS 正向搜索区域的功能是将域名解析为 IP 地址，Windows XP 系统中用于测试该功能的命令是______。

A. nslookup　　B. arp　　C. netstat　　D. query

14. 在 Linux 中，DNS 服务器的配置文件是_______。

A. /etc/hostname　　　　B. /etc/host.conf

C. /etc/resolv.conf　　　　D. /etc/httpd.conf

15. DNS 服务器中提供了多种资源记录，其中______定义了区域的邮件服务器及其优先级。

A. SOA　　B. NS　　C. PTR　　D. MX

16. 某 DHCP 服务器设置的地址池为 192.168.1.100 到 192.168.1.200，此时该网段下某台安装 Windows 系统的工作站启动后，获得的 IP 地址是 169.254.220.188，导致这一现象最可能的原因是________。

A. DHCP 服务器设置的租约期太长

B. DHCP 服务器提供了保留的 IP 地址

C. 网段上还有其他的 DHCP 服务器，这是工作站从其他的服务器上获得的地址

D. DHCP 服务器没有工作

17. 下列关于 DHCP 的说法中，错误的是________。

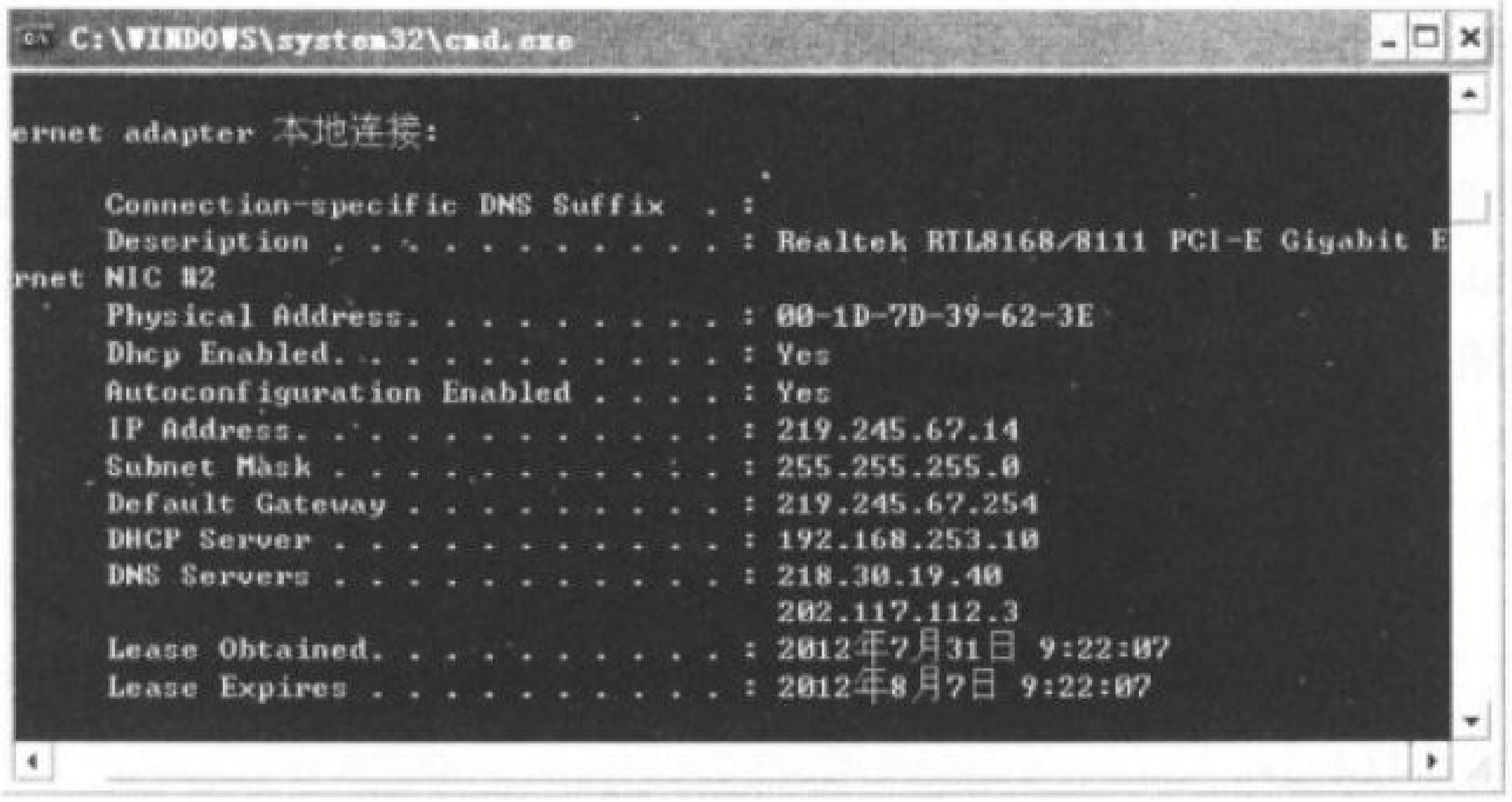
A. Windows 操作系统中，默认的租约期是 8 天

B. 客户机通常选择最先对应的 DHCP 服务器提供的地址

C. 客户机可以跨网段申请 DHCP 服务器提供的 IP 地址

D. 客户机一直使用 DHCP 服务器分配给它的 IP 地址，直到租约期结束才开始请求更新租约

18. 某主机本地连接属性如下图所示，下列说法中错误的是______。



A. IP 地址是采用 DHCP 服务自动分配的

B. DHCP 服务器的网卡物理地址为 00-1D-7D-39-62-3E

C. DNS 服务器地址可手动设置

D. 主机使用该地址的最大租约期为 7 天

19. Linux 系统中，DHCP 服务的主配置文件是__(1)__，保存客户端租约信息的文件是__(2)__。

(1)、(2)　A. dhcp.leases　　B. dhcp.conf　　C. xinetd.conf　　D. lease.conf

20. 在 Windows 环境下，DHCP 客户端可以使用______命令重新获得 IP 地址，这时客户机向 DHCP 服务器发送一个 dhcpdiscover 数据包来请求重新租用 IP 地址。

A. ipconfig/renew　　　　B. ipconfig/reload

C. ipconfig/release　　　　D. ipconfig/reset

21. 采用 DHCP 分配 IP 地址无法做到__(1)__，当客户机发送 dhcpdiscover 报文时采用__(2)__方式发送。

(1) A. 合理分配 IP 地址资源　　B. 减少网管员工作量
C. 减少 IP 地址分配出错可能　　D. 提高域名解析速度

(2) A. 广播　　B. 任意播　　C. 组播　　D. 单播

9.10.2 参考答案

1. C	2. D	3. B	4. D	5. D
6. B	7. D	8. B	9. A	10. B
11. A	12. B	13. A	14. C	15. D
16. C	17. D	18. B	19. (1) B (2) A	20. A
21. (1) D (2) A				

第 10 章　组 网 技 术

大纲要求：

- 交换机和路由器的配置，包括命令行接口配置、Web 方式访问交换机和路由器、VLAN、VOIP 配置、路由器的配置、广域联网、DTP、STP 和 RSTP。
- 远程访问服务器，包括功能和机制。
- 多层交换机功能和机制。
- IP 路由器功能和控制。

10.1　交换机和路由器

10.1.1　考点辅导

10.1.1.1　交换机基础

1. 交换机的分类

交换机的分类方式有如下几种。

(1) 按交换方式划分，可分为存储转发式交换机、直通式交换机和碎片过滤式交换机。

(2) 按交换的协议层划分，可分为工作在数据链路层的第二层交换机、工作在网络层的第三层交换机、工作在传输层的第四层交换机和多层交换机。

(3) 按交换机结构划分，可分为固定端口交换机和模块化交换机。

(4) 按配置方式划分，可分为堆叠型交换机和非堆叠型交换机。

(5) 按管理类型划分，可分为网管型交换机、非网管型交换机和智能型交换机。

(6) 按适用范围划分，可分为接入层交换机、汇聚层交换机和核心层交换机。

2. 交换机的性能指标

交换机的性能指标如下。

(1) 端口类型：双绞线端口、光纤端口、GBIC 端口、SFP 端口。

(2) 传输模式：半双工、全双工、全双工/半双工自适应。

(3) 包转发率：以单位时间内发送 64B 数据包的个数作为计算基准。

(4) 背板带宽：总带宽=端口数×端口速率×2(全双工模式)。

(5) MAC 地址数：交换机的 MAC 地址表中可以存储的 MAC 地址数量。

(6) VLAN 表项：最大 VLAN 数量反映了一台交换机所能支持的最大 VLAN 数目。

(7) 机架插槽数：机架式交换机所能安插的最大模块数。

10.1.1.2 路由器基础

1. 路由器的分类

从功能、性能和应用方面划分，路由器可分为骨干路由器、企业级路由器、接入级路由器。

(1) 骨干路由器是实现主干网络互联的关键设备。

(2) 企业级路由器连接许多终端，提供通信分类、优先级控制、用户认证等功能。

(3) 接入级路由器主要用于连接小型企业的客户群。

2. 路由器的端口

路由器与广域网连接的端口称为 WAN 端口，路由器与局域网连接的端口称为 LAN 端口。常见的网络端口有以下几种。

(1) RJ-45 端口：通过双绞线连接以太网。

(2) AUI 端口：用在令牌环网或总线型以太网中。

(3) 高速同步串口：用于连接 DDN、帧中继、X.25 和 PSTN 等网络。

(4) ISDN BRI 端口：通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。

(5) 异步串口：主要应用于与 Modem 或 Modem 池的连接。

(6) Console 端口：通过配置专用电缆连接至计算机串行口。

(7) AUX 端口：在远程配置时使用。

10.1.1.3 访问路由器和交换机

要对网络互联设备进行具体的配置首先就要有效地访问它们，一般来说可以用以下几种方法来访问路由器或交换机。

- 通过设备的 Console(控制台)端口接终端或运行终端仿真软件的微型计算机。
- 通过设备的 AUX 端口接 Modem，通过电话线与远方的终端或运行终端仿真软件的微机相连。
- 通过 Telnet 程序。
- 通过浏览器来访问。
- 通过网管软件。

下面以路由器为例给出几种访问路由器方法的连接图，如图 10-1 所示。

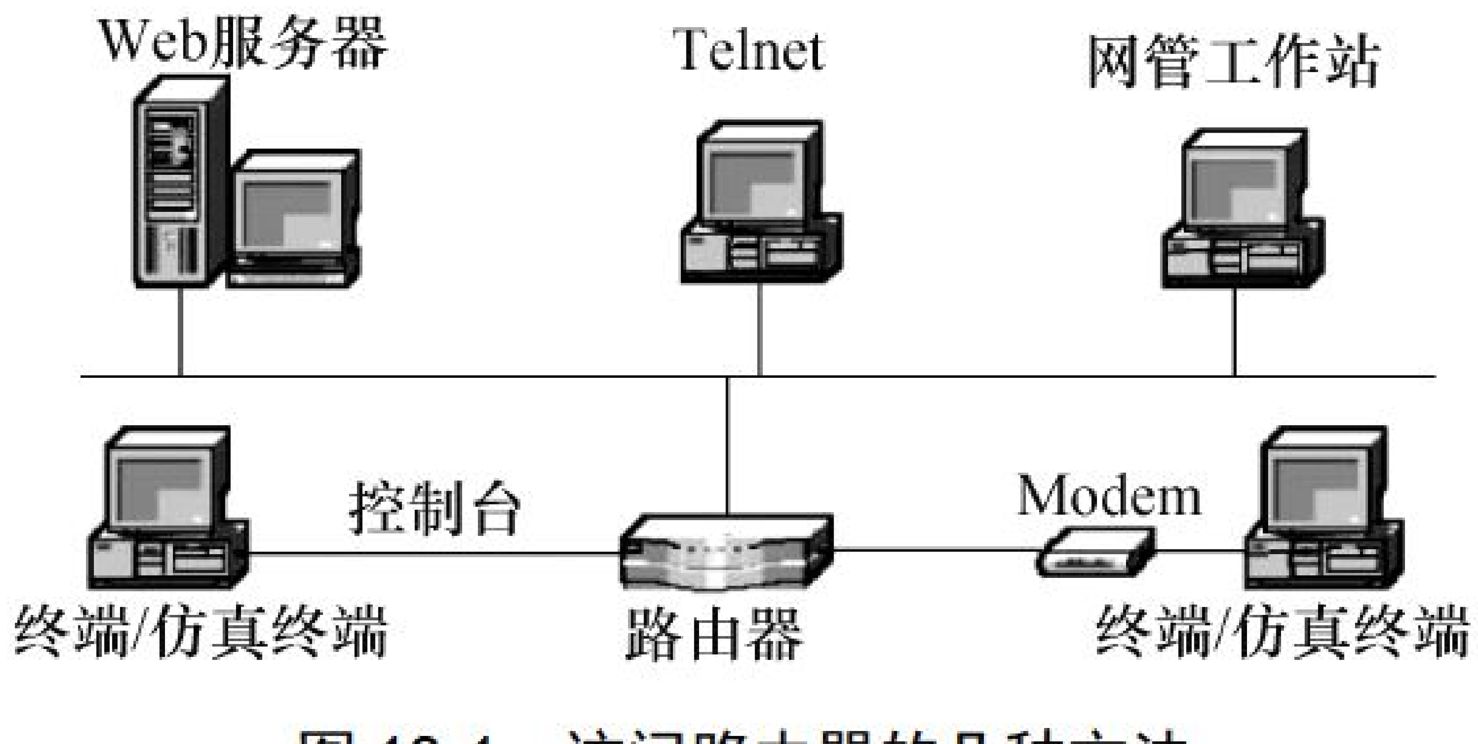


图 10-1 访问路由器的几种方法

路由器的第一次设置必须通过第一种方法来实现，同时第一种方法也是最常用、最直接有效的一种配置方法。因此，本书中对路由器和交换机的配置都是通过 Console 端口连

接运行超级终端仿真软件的 PC 来实现的。

Console 端口是路由器和交换机设备的基本端口，它是对一台新的路由器和交换机进行配置时必须使用的接口。连接 Console 端口的线称为控制台电缆(Console Cable)。在具体的连接上，Console 电缆一端插入网络设备的 Console 端口，另一端接入终端或 PC 的串行接口，从而实现对设备的访问和控制。

10.1.2　典型例题分析

例 10-1　观察交换机状态指示灯是初步判断交换机故障的检测方法，以下关于交换机状态指示灯的描述中，错误的是 (67) 。(2017 年下半年真题 67)

A. 交换机指示灯显示红色表明设备故障或者告警，需要关注和立即采取行动

B. STCK 指示灯显示绿色表示接口在提供远程供电

C. SYS 指示灯显示红色表明交换机可能存在风险或温度告警

D. 交换机业务接口对应单一指示灯，常亮表示连接，快闪表示数据传送

解析：STCK(STACK,堆叠)指示灯显示绿色表示业务指示灯暂时用来指示设备堆叠信息，即本设备为堆叠设备或堆叠从设备。

答案：B

例 10-2　两台交换机的光口对接，其中一台设备的光口 UP，另一台设备的光口 DOWN，定位此类故障的思路包括 (69) 。(2017 年下半年真题 69)

①光纤是否交叉对接。

②两端使用的光模块波长和速率是否一样。

③两端 COMB0 口是否都设置为光口。

④两个光口是否未同时配置自协商或者强制协商。

A. ①②③④　　B. ②③@　　C. ②③　　D. ①③④

解析：定位此类故障首先应查看光纤是否成对，存在不存在交叉对接的情况；其次通过命令行查看光模块参数，确定波长和速率是否相同；然后再通过命令行查看接口状态，端口工作模式是否都设置为光口模式；最后查看两个光口是否未同时配置自协商或强制协商。

答案：A

例 10-3　在默认配置时交换机所有端口 (62) ，不同 VLAN 的数据帧必须通过 (63) 传输。(2017 年上半年真题 62、63)

(62) A. 属于直通状态　　B. 属于不同 VLAN

C. 属于同一 VLAN　　D. 地址都相同

(63) A. DNS 服务器　　B. 路由器

C. 二层交换机　　D. DHCP 服务器

解析：默认情况下交换机的所有端口属于同一 VLAN，不同 VLAN 间的通信需要通过三层设备。

答案：(62) C　(63) B

例 10-4　以下关于交换机获取与其端口连接设备的 MAC 地址的叙述中，正确的是 (63) 。

(2015 年下半年真题 63)

A. 交换机从路由表中提取设备的 MAC 地址

B. 交换机检查端口流入分组的源地址

C. 交换机之间互相交换地址表

D. 由网络管理员手工输入设备的 MAC 地址

解析：交换机刚刚连接到以太网时，其转发表是空的。这时若交换机收到一个帧，它将怎样处理呢？交换机就按照以下自学习(self-learning)算法处理收到的帧(这样就逐步建立起转发表)，并且按照转发表把帧转发出去。这种自学习算法的原理并不复杂，因为：若从某个站 A 发出的帧从接口 x 进入了某交换机，那么从这个接口出发沿相反方向一定可以把一个帧传送到 A。所以交换机只要每收到一个帧，就记下其源地址和进入交换机的接口，作为转发表中的一个项目。

答案：B

10.1.3 同步练习

路由器通过光纤连接广域网的是______。

A. SFP 端口　　B. 同步串行口

C. Console 端口　　D. AUX 端口

10.1.4 同步练习参考答案

A

10.2 交换机的配置

10.2.1 考点辅导

10.2.1.1 交换机概述

交换机是一种具有简化、低价、高性能和高端口密集等特点的交换产品。交换机根据 OSI 层次通常可分为第二层交换机和多层交换机。通常所说的交换机就是指第二层交换机，也称为 LAN 交换机，如图 10-2 所示，它体现了桥接技术的复杂交换技术在 OSI 参考模型的第二层操作。与网桥一样，LAN 交换机按每一个包中的 MAC 地址相对简单的决策信息转发。这种转发决策一般不考虑包中隐藏的更深的其他信息。与网桥不同的是交换机转发延迟很小，操作接近单个局域网性能，远远超过了普通网桥互联网络之间的转发性能。

多层交换机与第二层交换机工作方式类似。除了使用第二层 MAC 地址进行交换外，多层交换机还使用第三层网络地址。传统上，第三层的功能只发生在路由器中，路由器依赖软件执行路由选择功能，实现对数据的存储和转发。随着硬件技术的发展，改良的硬件已经允许很多第三层路由选择功能出现在硬件中，进而出现了多层交换机。同时多层交换

机也可以检查第四层信息，包括帮助识别应用程序类型的 TCP 报头。

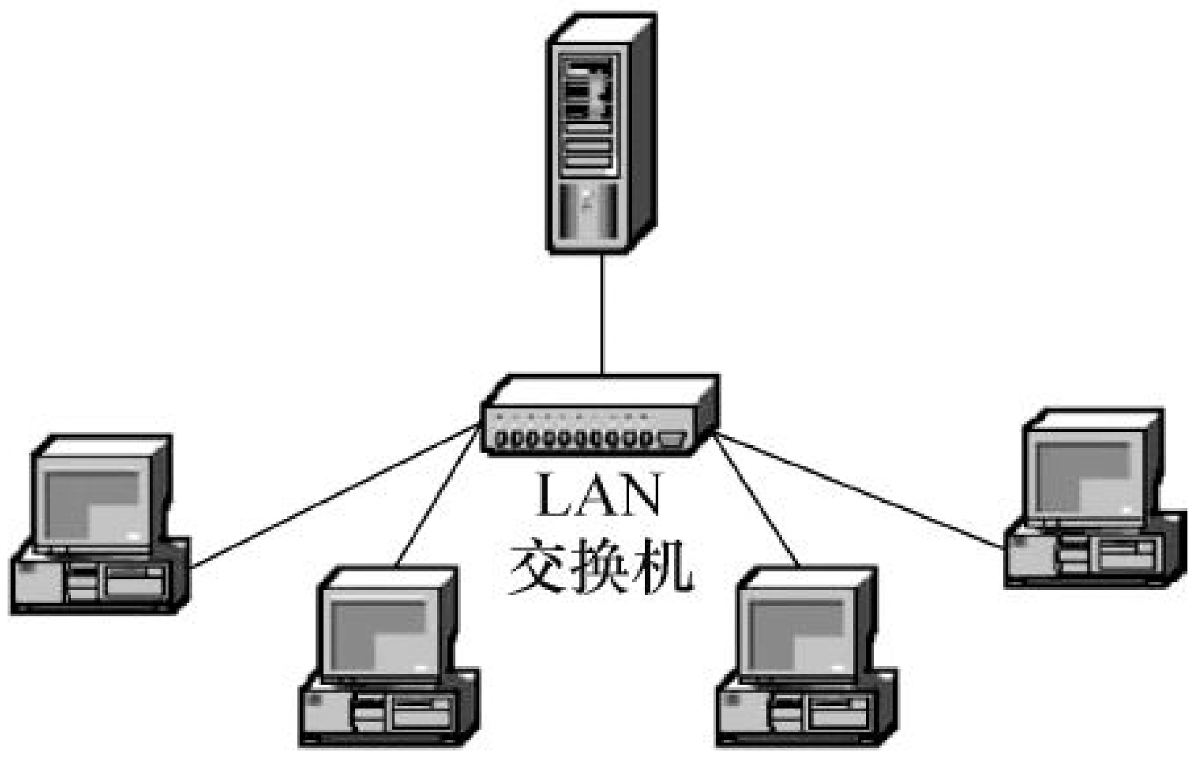


图 10-2　LAN 交换机

交换技术允许共享型和专用型的局域网段进行带宽调整，以减轻局域网之间信息流通出现的瓶颈问题。现在已有以太网、快速以太网、FDDI 和 ATM 技术的交换产品。类似传统的网桥，交换机提供了许多网络互联功能。交换机能经济地将网络分成小的冲突网域，为每个工作站提供更高的带宽。协议的透明性使得交换机在软件配置简单的情况下可以直接安装在多协议网络中；交换机使用现有的电缆、中继器、集线器和工作站的网卡，而不必做高层的硬件升级；交换机对工作站是透明的，这样管理开销低廉，简化了网络节点的增加、移动和网络变化的操作。

10.2.1.2　交换机的基本配置

下面以华为公司的 S5700 系列交换机为例，介绍交换机的一般配置过程。

1. 电缆连接及终端配置

如图 10-3 所示，接好 PC 机和交换机各自的电源线，在关机状态下，把 PC 机的串口 1(COM1)通过控制台电缆与交换机的 Console 端口相连，即完成设备的连接工作。

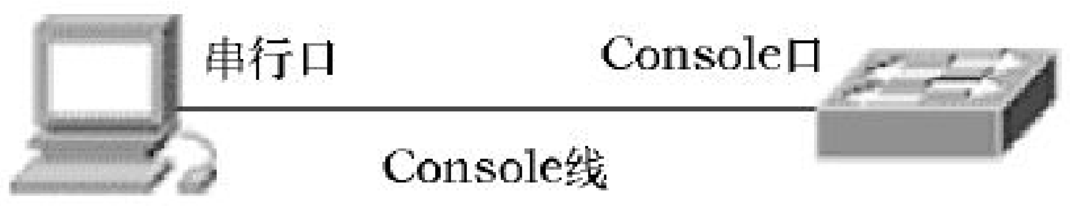


图 10-3　仿真终端与交换机的连接

交换机 Console 端口的默认参数如下。

端口速率：9600bps。

数据位：8。

奇偶校验码：无。

停止位：1。

流控：无。

在配置 PC 机的超级终端时只需保证端口属性的配置参数与上述参数相同匹配即可。以 Windows 环境下的 Hyper Terminal 为例配置 COM1 端口属性的对话框，如图 10-4 所示。

图 10-4 “COM1 属性”对话框

2. 交换机的启动

在配置好终端仿真软件后，终端窗口就会显示交换机的启动信息，显示交换机的版权信息和软件加载过程，直到出现提示用户设置登录密码。

```
BIOS loading …
…
Enter Password:
Confirm Password:
<HUAWEI>
```

完成 Console 登录密码设置后，用户便可以配置和使用交换机。

3. 交换机的基本配置

在默认配置下，所有接口处于可用状态，并且都属于 VLAN1，这种情况下交换机就可以正常工作了。但为了方便管理和使用，首先应对交换机做基本的配置。

(1) 配置交换机的设备名称、管理 VLAN 和 Telnet，在对网络中交换机进行管理时需要对交换机进行基本配置。

```
<HUAWEI>
<HUAWEI> system-view
[HUAWEI] vlan 5  //创建交换机管理 VLAN 5
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5
[HUAWEI-vlanif5] ip address 10.10.1.1 24
[HUAWEI-vlanif5] quit
[HUAWEI] telnet server enable   //Telnet 出厂时是关闭的，需要打开
[HUAWEI] user-interface vty 0 4  //Telnet 常用于设备管理员登录，推荐使用 AAA 认证
[HUAWEI-ui-vty0-4] protocol inbound telnet    //V2R6 及之前版本缺省支持 telnet
//协议，但是 V2R7 及之后版本缺省的是 SSH 协议，因此使用 telnet 登录之前，必须要先配置这
//条命令
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
```

```
[HUAWEI-aaa] local-user admin password irreversible-cipher Helloworld@6789
//配置管理员 Telnet 登录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin privilege level 15//将管理员的账号权限设置为 15(最高)
[HUAWEI-aaa]local-user admin service-type telnet
[HUAWEI-aaa]quit
[HUAWEI]quit
<HUAWEI>save
```

(2) 登录 Telent 到交换机，出现用户视图提示符。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1
//输入交换机管理 IP，并回车
Login authentication
Username:admin//输入用户名和密码
Password:
Info: The max number of VTY users is 5, and the number
of current VTY users on line is 1.
The current login time is 2014-05-06 18:33:18+00:00.
<HUAWEI>
```

(3) 配置交换机的接口。交换机的接口属性默认支持一般网络环境，一般情况下是不需要对其接口进行设置的。在某些情况下需要对其端口属性进行配置时，配置的对象主要有接口隔离、速率、双工等信息。

```
#配置接口 GE1/0/1 和 GE1/0/2 的端口隔离功能，实现两个接口之间的二层数据隔离，三层数据互通
<Switch1>system-view
[Switch1]port-isolate mode 12
[Switch1]interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1]port-isolate enable group 1
[Switch-GigabitEthernet1/0/1]quit
[Switch1]interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2]port-isolate enable group 1
[Switch-GigabitEthernet1/0/2]quit

#配置以太网接口 GE0/0/1 在自协商模式下协商速率为 100Mb/s
<Switch1>system-view
[Switch1] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1]negotiation auto
[Switch-GigabitEthernet1/0/1]auto speed 100

#配置以太网接口 GE0/0/1 在自协商模式下双工模式为全双工模式
<Switch1>system-view
[Switch1] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1]negotiation auto
```

(4) 查看和配置 MAC 地址表。交换机通过学习网络中设备的 MAC 地址，并将学习得到的 MAC 地址存放在交换机的缓存中。在需要向目标地址发送数据时就从 MAC 地址表中查找相应的地址，找到后才可以向目标快速发送数据。

MAC 表由多条 MAC 地址表项组成。MAC 地址表项由 MAC、VLAN 和端口组成，交换机在收到数据帧时，会解析出数据帧的源 MAC 地址和 VLAN ID 并与接收数据帧的端口组合成一条数据表项。MAC 地址表项的查看可以了解交换机运行的状态信息，排查故障。

```
#执行命令 display mac-address，查看所有的 MAC 地址表项
<Switch1>display mac-address
------------------------------------------------------------------------
MAC Address     VLAN/VSI           Learned-From            Type
------------------------------------------------------------------------
00e0-0900-7890  10/-               -                      black
00e0-0230-1234  20/-               GE1/0/1                 static
0001-0002-0003  30/-               Eth-Trunk1              dynamic
------------------------------------------------------------------------
Total items displayed = 3

#执行命令 display interface vlanif5，显示 VLANIF 接口的 MAC 地址
<Switch1>display interface vlanif5
Vlanif5 current state:DOWN
Line protocol current state:DOWN
Description:
Route Port,Address is 192.168.1.1/24
IP Sending Frames'Format is PKTFMT_ETHNT_2,Hardware address is
00e0-0987-7891
Current system time:2016-07-03 13:33:09+08:00
        Input bandwidth utilization :--
        Output bandwidth utilization :--
#在 MAC 地址表中增加静态 MAC 地址表项，目的 MAC 地址为 0001-0002-0003，VLAN 5 的报文，
从接口 gigabitethernet0/0/5 转发出去
[Switch1]mac-address static 0001-0002-0003 gigabitethernet 0/0/5 vlan 5
```

10.2.1.3 配置和管理 VLAN

VLAN 技术是交换技术的重要组成部分，也是交换机配置的基础。它用于把物理上直接相连的网络从逻辑上划分为多个子网。每一个 VLAN 对应着一个广播域，处于不同 VLAN 上的主机不能进行通信，不同 VLAN 之间的通信要引入第三层交换技术才可以解决。对虚拟局域网的配置和管理主要涉及链路和接口类型、GARP 协议和 VLAN 的配置。

链路和接口类型，为了适应不同网络环境的组网需要，链路类型分为接入链路(Access Link)和干道链路(Trunk Link)。接入链路只能承载 1 个 VLAN 的数据帧，用于连接交换机和用户终端；干道链路能承载多个不同 VLAN 的数据帧，用于交换机间互连或连接交换机与路由器。根据接口连接对象以及对收发数据帧处理的不同，以太网接口分为 Access 接口、Trunk 接口、Hybrid 接口和 QinQ 接口四种接口类型，分别用于连接终端用户、交换机与路由器以及公网与私网的互联等。

GARP 协议主要用于建立一种属性传递扩散机制，以保证协议实体能够注册和注销该属性。简单说就是为了简化网络中配置 VLAN 的操作，通过 GVRP 的 VLAN 自动注册功能将设备上的 VLAN 信息快速复制到整个交换网，达到减少手工配置及保证 VLAN 配置正确的

目的。

交换机的初始状态是工作在透明模式，有一个默认的 VLAN1，所有端口都属于 VLAN1。

1. 划分 VLAN 的方法

虚拟局域网是交换机的重要功能，通常虚拟局域网的实现形式有多种，分别是基于接口、MAC 地址、子网、网络层协议、匹配策略方式来划分 VLAN。

通过接口来划分 VLAN。交换机的每个接口配置不同的 PVID，当数据帧进入交换机时没有带 VLAN 标签，该数据帧就会被打上接口指定 PVID 的 Tag 并在指定 PVID 中传输。

通过源 MAC 地址来划分 VLAN。建立 MAC 地址和 VLAN ID 映射关系表，当交换机收到的是 Untagged 帧时，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过子网划分 VLAN。建立 IP 地址和 VLAN ID 映射关系表，当交换机收到的是 Untagged 帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过网络层协议划分 VLAN。建立以太网帧中的协议域和 VLAN ID 的映射关系表，当收到的是 Untagged 帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过策略匹配划分 VLAN，实现多种组合的划分，包括接口、MAC 地址、IP 地址等。建立配置策略，当收到的是 Untagged 帧，且匹配配置的策略时，给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

2. 配置 VLAN 举例

在网络中，用于终端与交换机、交换机与交换机、交换机与路由器连接时 VLAN 的划分方式多种多样，需要灵活运用。这里就接入层交换机的 VLAN 划分举例说明。

(1) 以接入交换机 ACC1 为例，创建 ACC1 的业务 VLAN10 和 20。

```
<HUAWEI> system-view
[HUAWEI] sysnameACC1//修改设备名称为 ACC1
[ACC1] vlan batch 10 20//批量创建 VLAN
```

(2) 配置 ACC1 连接 CORE1 和 CORE2 的 GE0/0/3 和 GE0/0/4，透传部门 A 和部门 B 的 VLAN。

```
[ACC1] interface GigabitEthernet 0/0/3
[ACC1-GigabitEthernet0/0/3] port link-type trunk
//配置为 trunk 模式，用于透传 VLAN
[ACC1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
//配置 GE0/0/3 透传 ACC1 上的业务 VLAN
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4
[ACC1-GigabitEthernet0/0/4] port link-type trunk
//配置为 trunk 模式，用于透传 VLAN
[ACC1-GigabitEthernet0/0/4] port trunk allow-pass vlan 10 20
//配置 GE0/0/4 透传 ACC1 上的业务 VLAN
[ACC1-GigabitEthernet0/0/4] quit
```

(3) 配置 ACC1 连接用户的接口，使各部门加入 VLAN。

```
[ACC1] interfaceGigabitEthernet0/0/1 //配置连接部门 A 的接口
[ACC1-GigabitEthernet0/0/1] port link-type access
[ACC1-GigabitEthernet0/0/1] port default vlan 10
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interfaceGigabitEthernet0/0/2 //配置连接部门 B 的接口
[ACC1-GigabitEthernet0/0/2] port link-type access
[ACC1-GigabitEthernet0/0/2] port default vlan 20
[ACC1-GigabitEthernet0/0/2] quit
```

(4) 配置 BPDU 保护功能，加强网络的稳定性。

```
[ACC1] stpbpdu-protection
```

如果把 ACC1 下接入的用户都加入 VLAN 10，为了配置简单，也可以 ACC1 上不配置 VLAN，而把 CORE1、CORE2 与 ACC1 直接相连的接口以 access 方式加入 VLAN10，这样通过 ACC1 接入的用户全部属于 VLAN10。

3. 将端口加入到某个 VLAN 中

首先进入端口配置模式，执行 switchport mode access 命令设置端口为静态 VLAN 访问模式，然后执行 switchport access vlan vlan_id 命令将端口分配给可信的 VLAN。

10.2.1.4 生成树协议配置

生成树负载均衡实现方法如下。

(1) 使用 STP 端口权值实现。

(2) 使用 STP 路径值实现。

10.2.2 典型例题分析

例 10-5 关于为华为交换机设置密码，正确的说法是 (66) 。(2017 年下半年真题 66)

①华为交换机的默认用户名是 admin，无密码。

②通过 BootRoom 可以重置 Console 口密码。

③ telnet 登录密码丢失，通过 Console 口登录交换机后重新进行配置。

④通过 Console 口登录交换机重置 BootRoom 密码。

A. ①②③④　　B. ②③④　　C. ②③　　D. ①③④

解析：华为交换机可以通过 Telnet 登录交换机修改 Console 口密码；也可以通过 BootRoom 清除 Console 口密码后再修改；若 Telnet 密码或 Web 密码丢失，可以通过 Console 口登录交换机后重新进行配置；若 BootRoom 密码丢失，可以通过 Console 口登录交换机后重置。华为设备的 Web 登录界面默认用户名是 admin，而从 Console 口进入的用户没有默认用户名。

答案：C

例 10-6 下面的交换机命令中， (59) 为端口指定 VLAN。(2016 年下半年真题 59)

A. S1(config-if)#vlan-membership static　　B. S1(config-if)#vlan database

C. S1(config-if)#switchport mode access　　　　D. S1(config-if)#switchport access vlan 1

解析：在默认配置下，所有的接口都处于可用状态且均属于 VLAN1，采用静态配置法配置 VLAN，也就是说在交换机上手动将某个端口分配给一个 VLAN。所用命令为 S1(config-if)#switchport access vlan 1。

答案：D

例 10-7　以下关于以太网交换机地址学习机制的说法中，错误的是__(12)__。(2016 年上半年真题 12)

A. 交换机的初始 MAC 地址表为空

B. 交换机接收到数据帧后，如果没有相应的表项，则不转发该帧

C. 交换机通过读取输入帧中的源地址添加相应的 MAC 地址表项

D. 交换机的 MAC 地址表项是动态变化的

解析：交换机接收到数据帧后，如果没有相应的表项，将广播发送帧。

答案：B

10.2.3　同步练习

1. 把交换机由特权模式转换到全局配置模式使用的命令是________。

   A. interface f0/1　　B. config terminal　　C. enable　　D. no shutdown

2. 以下的命令中，可以为交换机配置默认网关地址的是______。

   A. 2950(config)# default-gateway 192.1610.1.254

   B. 2950(config-if)# default-gateway 192.1610.1.254

   C. 2950(config)#ip default-gateway 192.1610.1.254

   D. 2950(config-if)#ip default-gateway 192.1610.1.254

3. 交换机命令 switch(config)#vtp pruning 的作用是________。

   A. 指定交换机的工作模式　　　　B. 启用 VTP 静态修剪

   C. 指定 VTP 域名　　　　　　　D. 启动 VTP 动态修剪

4. 能进入 VLAN 配置状态的交换机命令是________。

   A. 2950(config)# vtp pruning　　　　B. 2950# vlan database

   C. 2950(config)# vtp server　　　　D. 2950(config)# vtp mode

5. 交换机命令 Switch>enable 的作用是________。

   A. 配置访问口令　　　　B. 进入配置模式

   C. 进入特权模式　　　　D. 显示当前模式

6. 新交换机出厂时的默认配置是________　。

   A. 预配置为 VLAN1，VTP 模式为服务器

   B. 预配置为 VLAN1，VTP 模式为客户机

   C. 预配置为 VLAN0，VTP 模式为服务器

   D. 预配置为 VLAN0，VTP 模式为客户机

10.2.4 同步练习参考答案

1. B　　2. C　　3. D　　4. B　　5. C　　6. A

10.3 路由器的配置

10.3.1 考点辅导

10.3.1.1 路由器概述

路由器是一种典型的网络层设备。在 OSI 参考模型中被称为中继系统，完成网络层中继或第三层中继的任务。路由器负责在两个局域网的网络层间接传输数据分组，并确定网络上数据传送的最佳路径。也因为它们运行 IP 基于第三层信息来为分组选择路由，如图 10-5 所示，所以路由器已经成为 Internet 的骨干。

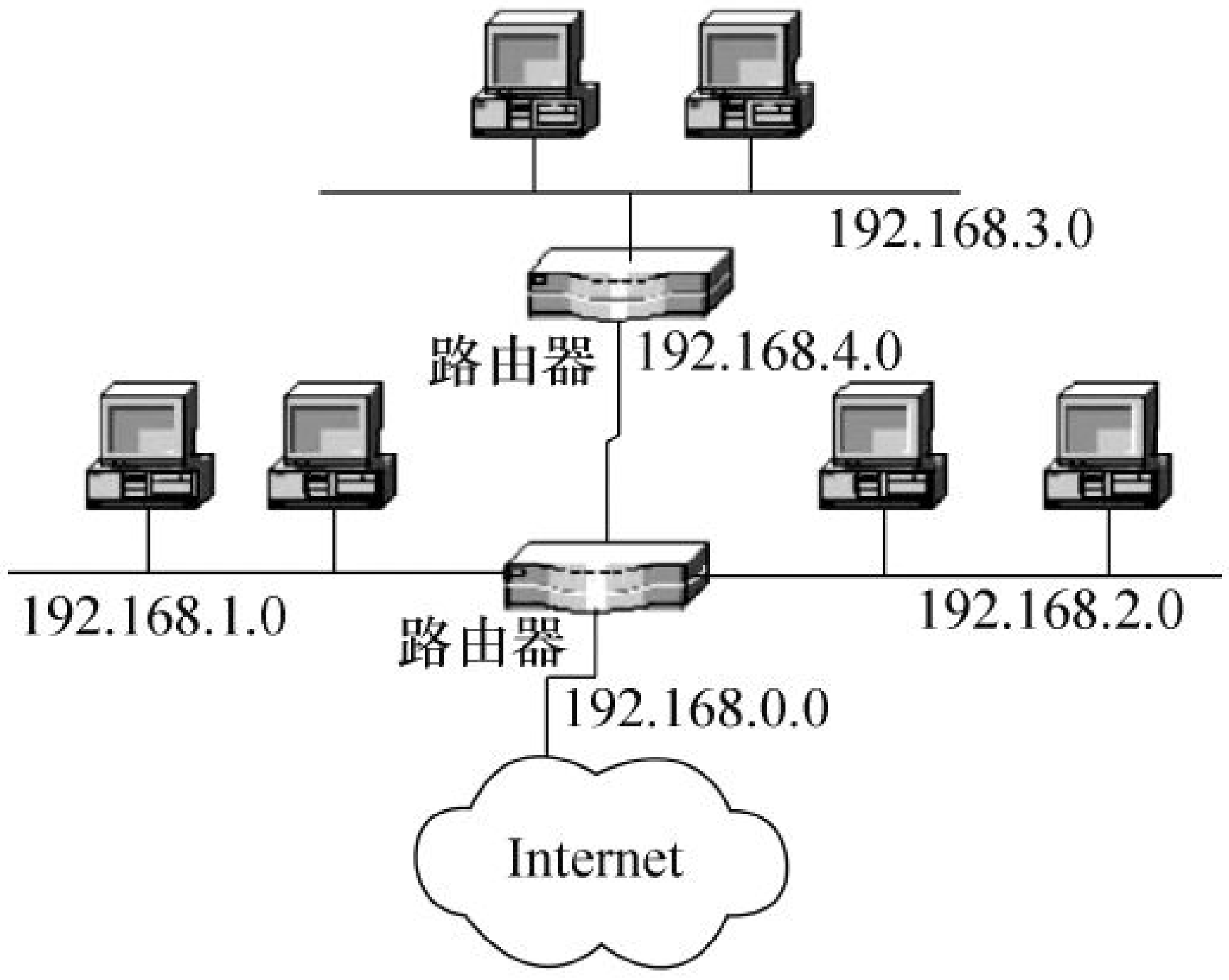


图 10-5　路由器

路由器用于连接多个逻辑上分开的网络。逻辑网络是代表一个单独的网络或者一个子网。当数据从一个子网传输到另一个子网时，可通过路由器来完成。因此，路由器具有判断网络地址和选择路径的功能，它能在多网络互联环境中建立灵活的连接，可用完全不同的数据分组和介质访问方法连接各种子网。它不关心各子网使用的硬件设备，但要求运行与网络层协议一致的软件。路由器分本地路由器和远程路由器，本地路由器是用来连接网络传输介质的，如光纤、同轴电缆、双绞线；远程路由器是用来连接远程传输介质的，并要配置适当的联网设备，如电话线要配置调制解调器，无线传输要配置无线接收机、发射机等。

一般来说，异种网络互联与多个子网互联都应采用路由器来完成。

路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据帧有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表(Routing Table)，供路由选择时使用。路由表中保存着子网的标志信息、网上路由器的个数和下一个

路由器的名字等内容。路由表可以是由系统管理员固定设置好的；可以由系统动态修改；可以由路由器自动调整；也可以由主机控制。

由系统管理员事先设置好的固定的路由表称为静态(Static)路由表，一般是在系统安装时就根据网络的配置情况预先设定的，它不会随未来网络结构的改变而改变。

动态(Dynamic)路由表是路由器根据网络系统的运行情况而自动调整的路由表。路由器根据路由选择协议(Routing Protocol)提供的功能，自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

10.3.1.2　路由器的基本配置

1. 路由器的命令状态

与交换机的配置类似，路由器的配置操作有 3 种模式，即用户视图、系统视图和具体业务视图。用户视图模式下，用户可以完成查看运行状态和统计信息等功能，这些命令对路由器的正常工作没有影响；在系统视图模式下，用户可以配置系统参数以及通过该视图进入其他的功能配置视图；在具体业务视图模式下，用户可以配置接口相关的物理属性、链接层特性及 IP 地址等重要参数，路由协议的大部分参数也需要在这种模式下配置。其中，配置模式又分为全局配置模式、接口配置模式、路由协议配置模式、线路配置模式等子模式。在不同的工作模式下，路由器有不同的命令提示状态。

<Switch>。在交换机正常启动后，用户使用终端仿真软件或 Telent 登录交换机，可自动进入用户配置模式，这时用户可以查看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。

[Switch]。路由器处于系统视图命令状态，在<Switch>提示符下输入 system-view，可进入系统视图状态，这时不仅可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

[Switch-vlan]。路由器处于具体的业务视图状态，在[Switch]提示符下输入需要配置的业务命令，可进入该状态。退出具体的业务输入 quit。

在开机自检时，按 Ctrl+Break 组合键可进入 BootROM menu 状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导，或者进行路由器口令恢复时要进入该状态。

2. 路由器的基本配置

配置 enable 口令、enable 密码和主机名。在路由器中同样可以配置启用口令(enable password)和启用密码(enable secret)，一般情况下只需配置一个就可以，当两者同时配置时，后者生效。这两者的区别是启用口令以明文显示，而启用密码以密文形式显示。主机名及路由器口令的设置和上一节对交换机配置的主机名及口令相同，这里不再赘述。

配置路由器以太网接口。路由器一般提供一个或多个以太网接口槽，每个槽上会有一个以上以太网接口。以太网接口因此而命名为{Ethernet 槽位/端口}或{GigabitEthernet 槽位/端口}，例如 Ethernet0/0、GigabitEthernet0/0/1，也可缩写为 Eth0/0、GE0/0/1。

对以太网接口做如下配置：

```
#设置系统的日期、时间和时区
<Huawei>clock timezone BJ add 08:00:00
<Huawei>clock datetime 20:10:00 2015-03-26
```

```
#设置设备名称和管理 IP 地址
<Huawei>system-view
[Huawei]sysname Server
[Server]interface gigabitethernet 0/0/0
[Server-GigabitEthernet0/0/0]ip address 10.137.217.177 24
[Server-GigabitEthernet0/0/0]quit

#设置 Telnet 用户的级别和认证方式
[Server] telent server enable
[Server] user-interface vty 0 4
[Server-ui-vty0-4]user privilege level 15
[Server-ui-vty0-4]authentication-mode aaa
[Server-ui-vty0-4]quit
[Server]aaa
[Server-aaa] local-user admin1234 password irreversible-cipher
Helloworld@6789
[Server-aaa] local-user admin1234 privilege level 15
[Server-aaa] local-user admin1234 service-type telent
[Server-aaa]quit
```

由于同一厂商的网络设备往往采用一种网络操作平台，交换机、路由器的配置以及命令的使用都是相似的。

3. 批量配置技术

大型网络的组网和网络管理中都会同时用到多个路由器和交换设备，可以通过批量配置技术快速配置多台网络设备。例如，华为交换机 AR 系列路由器通过 Auto-Config 功能实现设备的批量配置，Auto-Config 是指新出厂或空配置设备加电启动时采用的一种自动加载版本文件(包括系统软件、补丁文件、配置文件)的功能。

如图 10-6 所示，RouterA、RouterB 和 RouterC 运行 Auto-Config 功能后，设备作为 DHCP 客户端定时向 DHCP 服务器发送 DHCP 请求报文以获得配置信息，然后 DHCP 服务器向待配置设备响应 DHCP 应答报文，报文内容包括分配给待配置设备的 IP 地址、文件服务器的 IP 地址、文件服务器的登录方式、版本文件的配置信息(此信息也可以通过中间文件获取，中间文件需要预先编辑存放在文件服务器)，最后设备根据收到的 DHCP 响应报文中携带的配置信息，从指定的文件服务器自动获取版本文件，并设置为下次启动加载的文件，待设备重启后，设备就实现了版本文件的自动加载。

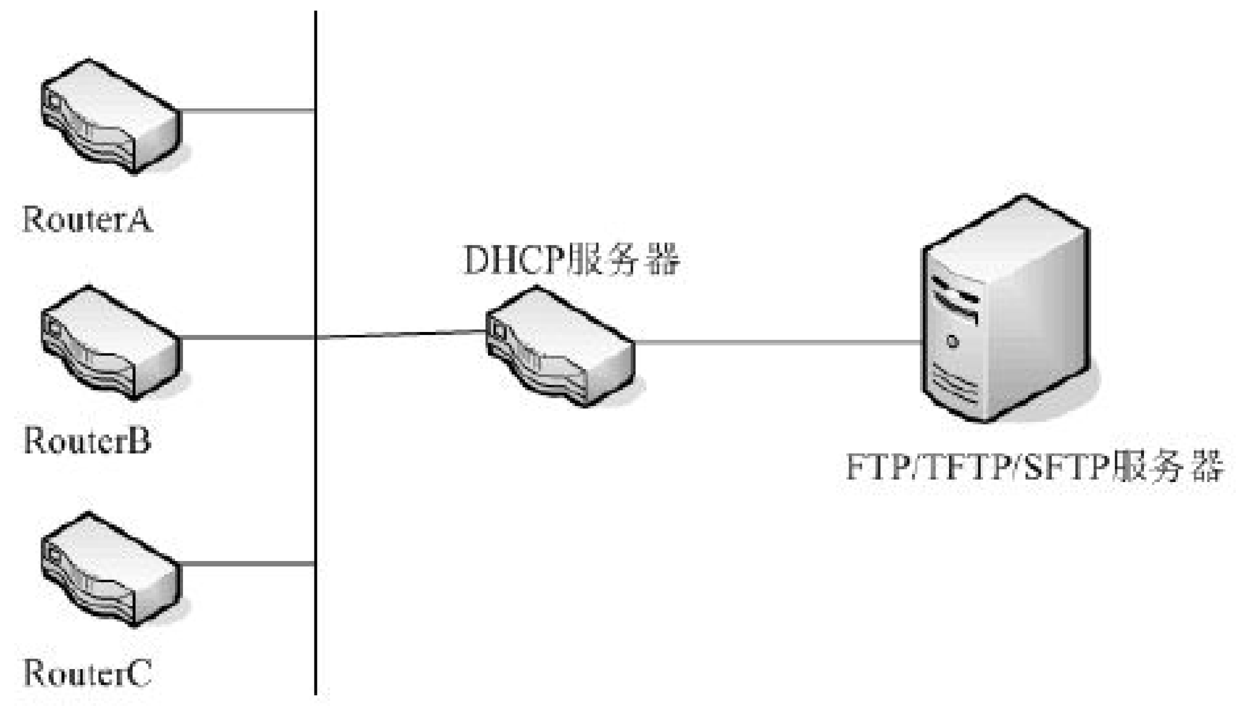


图 10-6　批量配置

若网络中有一台 SFTP 服务器(GE0/0/1，IP 地址 172.16.100.100/24)，一台 DHCP 服务器(GE0/0/1，IP 地址 172.16.100.1/24 用于与 SFTP 互联；Eth1/0/1-3，VLANIF10，IP 地址 172.16.200.100/24 用于与待配置路由器互联)，3 台待配置路由器。举例说明配置同网段 Auto-Config 步骤。

步骤 1：配置 SFTP 服务器。

```
#配置 SFTP 服务器功能及参数
<Huawei> system-view
[Huawei] sysname SFTP Server
[SFTP Server] rsa local-key-pair create the key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512~2048).
NOTES: If the key modulus is less than 2048,
It will introduce potential secunty risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys…
..........................................................................................
[SFTP Server] sftp server enable

#配置 SSH 用户登录的用户界面
[SFTP Server] user-interface vty 0 4
[SFTP Server-ui-vty0-4] authentication-mode aaa
[SFTP Server-ui-vty0-4] protocol inbound all
[SFTP Server-ui-vty0-4] user privilege level 15
[SFTP Server-ui-vty0-4] quit

#配置 SSH 用户
[SFTP Server] aaa
[SFTP Server-aaa] local-user user password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters,
including lowercase letters, uppercase letters, numerals and special
characters.
Please entes password:
Please confirm password:
[SFTP Server-aaa] local-user user privilege level 15
[SFTP Server-aaa] local-user user service-type ssh
[SFTP Server-aaa] local-user user ftp-directory flash:\autoconfig
[SFTP Server-aaa] quit
[SFTP Server] ssh user user authentication-type password

#配置 SFTP 服务器的 IP 地址
[SFTP Server] interface gigabitethernet 0/0/1
[SFTP Server-GigabitEthernet0/0/1] ip address 172.16.100.100 255.255.255.0
[SFTP Server-GigabitEthernet0/0/1 quit

#在 SFTP 服务器上配置缺省路由
```

```
[SFTP Server] ip route-static 0.0.0.0 0.0.0.0 172.16.100.1
```

步骤 2：将配置文件、系统软件和补丁文件上传至 SFTP 服务器的工作目录 flash:\autoconfig 上(上传步骤略)。

步骤 3：配置 DHCP 服务器(以 AR2220 为例)。

```
<Huawei> system-view
[Huawei] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] vlan 10
[DHCP Server-vlan10] quit
[DHCP Server] interface ethernet 1/0/1
[DHCP Server-Ethernet1/0/1] port link-type hybrid
[DHCP Server-Ethernet1/0/1] port hybrid untagged vlan 10
[DHCP Server-Ethernet1/0/1] port hybrid pvid vlan 10
[DHCP Server-Ethernet1/0/1] quit
[DHCP Server] interface ethernet 1/0/2
[DHCP Server-Ethernet1/0/2] port link-type hybrid
[DHCP Server-Ethernet1/0/2] port hybrid untagged vlan 10
[DHCP Server-Ethernet1/0/2] port hybrid pvid vlan 10
[DHCP Server-Ethernet1/0/2] quit
[DHCP Server] interface Ethernet 1/0/3
[DHCP Server-Ethernet1/0/3] port link-type hybrid
[DHCP Server-Ethernet1/0/3] port hybrid untagged vlan 10
[DHCP Server-Ethernet1/0/3] port hybrid pvid vlan 10
[DHCP Server-Ethernet1/0/3] quit
[DHCP Server] interface gigabitEthernet 0/0/1
[DHCP Server-GigabitEthernet0/0/1] ip address 172.16.100.1 255.255.255.0
[DHCP Server-GigabitEthernet0/0/1] quit
[DHCP Server] interface vlanif 10
[DHCP Server-Vlanif10] ip address 172.16.200.100 255.255.255.0
[DHCP Server-Vlanif10] dhcp select global
[DHCP Server-Vlanif10] quit
[DHCP Server] ip pool auto-config
[DHCP Server-ip-pool-auto-config] network 172.16.200.0 mask 255.255.255.0
[DHCP Server-ip-pool-auto-config] gateway-list 172.16.200.100
[DHCP Server-ip-pool-auto-config] option 67 ascii ar_V200R008
(C20&C30) .cfg
[DHCP Server-ip-pool-auto-config] option 141 ascii user
[DHCP Server-ip-pool-auto-config] option 142 cipher Huawei@123
[DHCP Server-ip-pool-auto-config] option 143 ip-address 172.16.100.100
[DHCPServer-ip-pool-auto-config]option145ascii vrpfile=auto_V200R008
(C20&C30) .cc;vrpver=V200R008 (C20&C30) ;patchfile=ar_V200R008
(C20&C30) .pat;
[DHCP Server-ip-pool-auto-config] quit
```

步骤 4：待配置设备 RouterA、RouterB 和 Router C 上电启动，Auto-Config 流程开始运行。

步骤 5：检查配置结果。

```
# Auto-Config 流程结束后，登录到待配置设备执行命令 display startup 查看设备当前的启
动系统软件，启动配置文件和启动补丁文件
以 RouterA 为例：
<Huawei> display startup
MainBoard:
Startup system software:              flash:/ar_V200R008 (C20&C30) .cc
Next startup system software:             flash:/ar_V200R008 (C20&C30) .cc
Backup system software for next startup:    null
Startup saved-configuration file:          flash:/ar_V200R008
(C20&C30) .cfg
Next startup saved-configuration file       flash:/ar_V200R008
(C20&C30) .cfg
Startup license file:                     null
Next startup license file:                  null
Startup patch package:                    flash:/ar_V200R008 (C20&C30) .pat
Next startup patch package:               flash:/ar V200R008 (C20&C30) .pat
Startup voice-files:                      null
Next startup voice-files:                   null
```

4. 配置静态路由

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径，网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

1)　IPv4 静态路由设置

在创建静态路由时，可以同时指定出接口和下一跳。对于不同的出接口类型，也可以只指定出接口或只指定下一跳。

- 对于点到点接口，指定出接口。
- 对于 NBMA(Non Broadcast Multiple Access)接口，指定下一跳。
- 对于广播接口(如以太网接口)，指定下一跳。

在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担；如果指定不同优先级，则可实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv4 静态缺省路由。缺省情况下，没有创建 IPv4 静态缺省路由。

操作步骤如下。

(1)　执行命令 system-view，进入系统视图。

(2)　配置 IPv4 静态路由。

①　在公网上配置 IPv4 静态路由：

```
ip route-static ip-address { mask | mask-length } { nexthop-address |
interface-type interface-number [ nexthop-address ] | vpn-instance
vpn-instance-name nexthop-address } [ preference preference | tag tag ] *
[ description text ]
```

②　在 VPN 实例中配置 IPv4 静态路由：

```
ip route-static vpn-instance vpn-source-name destination-address { mask |
mask-length } { nexthop-address [ public ] | interface-type interface-number
```

```
[ nexthop-address ] | vpn-instance vpn-instance-name nexthop-address }
[ preference preference | tag tag ] * [ description text ]
```

2) IPv6 静态路由设置

在创建静态路由时，可以同时指定出接口和下一跳。对于不同的出接口类型，也可以只指定出接口或只指定下一跳。

- 对于点到点接口，指定出接口。
- 对于 NBMA(Non Broadcast Multiple Access)接口，指定下一跳。
- 对于广播类型接口，指定出接口。如果也指定下一跳，下一跳地址可以不是链路本地地址。

在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担；如果指定不同优先级，则可实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv6 静态缺省路由。缺省情况下，没有创建 IPv6 静态缺省路由。

操作步骤如下。

(1) 执行命令 system-view，进入系统视图。

(2) 配置 IPv6 静态路由。

① 在公网上配置 IPv6 静态路由：

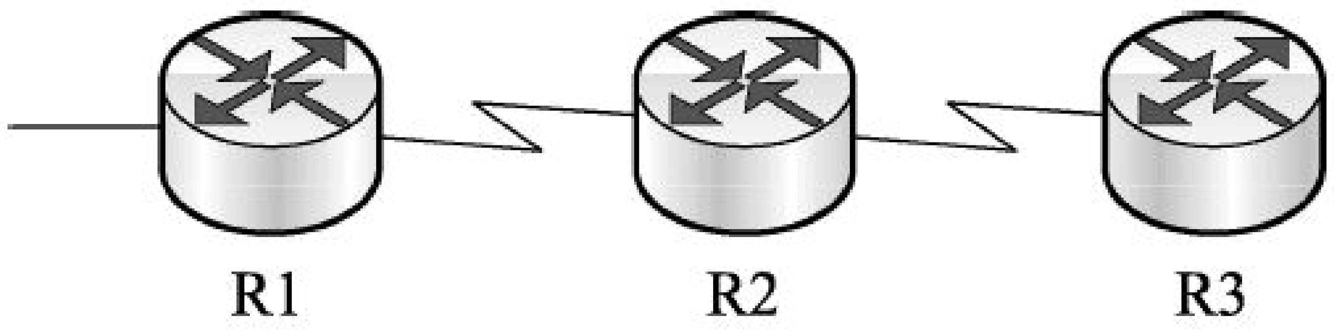
```
ipv6 route-static dest-ipv6-address prefix-length { interface-type
interface-number [ nexthop-ipv6-address ] | nexthop-ipv6-address }
[ preference preference | tag tag ] * [ description text ]
```

② 在 VPN 实例中配置 IPv6 静态路由：

```
ipv6 route-static vpn-instance vpn-instance-name dest-ipv6-address
prefix-length { [ interface-type interface-number ] nexthop-ipv6-address |
nexthop-ipv6-address [ public ] | vpn-instance vpn-destination-name
nexthop-ipv6-address } [ preference preference | tag tag ] * [ description
text ]
```

10.3.2 典型例题分析

例 10-8 运行 RIPv2 的 3 台路由器按照如下图所示的方式连接，路由表项最少需经过__(57)__可达到收敛状态。(2017 年上半年真题 57)



A. 30s　　B. 60s　　C. 90s　　D. 120s

解析：RIP 的特点：①只和相邻路由器交换信息；②交换的信息是本路由器知道的所有信息，也就是路由表；③每隔 30s 发整张路由表的副表到邻居路由器。在本题中，经过 60s 的时候所有路由器就能学到所有的网段信息。

答案：B

例 10-9　连接终端和数字专线的设备 CSU/DSU 被集成在路由器__(19)__中。(2016 年下半年真题 19)

A. RJ-45 端口　　B. 同步串口　　C. AUI 端口　　D. 异步串口

解析：通道服务单元／数据服务单元(CSU/DSU)是用于连接终端和数字专线的设备，而且 CSU/DSU 属于 DCE(Data Communication Equipment，数据通信设备)。目前 CSU/DSU 通常都被集成在路由器的同步串口之中，通常 CSU/DSU 被整合在一起，是一个硬件设备。

答案：B

例 10-10　如果路由器显示"Serial 1 is down, line protocol is down"故障信息，则问题出在 OSI 参考模型的__(58)__。(2016 年下半年真题 58)

A. 物理层　　B. 数据链路层　　C. 网络层　　D. 会话层

解析：接口信息显示"Serial l is down, line protocol is down"，其中第一个 down 是物理层状态，第二个 down 是数据链路层状态，该信息说明物理层故障进而导致 line protocol down 掉了，并不能判定 line protocol 是否真正 down 了。故答案为 A。

答案：A

例 10-11　路由器包含多种端口以连接不同类型的网络设备，其中能够连接 DDN、帧中继、X. 25 和 PSTN 等广域网络的是__(13)__。(2016 年上半年真题 13)

A. 同步串口　　B. 异步串口　　C. AUX 端口　　D. Consol 端口

解析：常见的路由器端口如下。

RJ-45 端口：通过双绞线连接以太网。

AUI 端口：用在令牌环网或总线型以太网中。

高速同步串口：用于连接 DDN、帧中继、X.25 和 PSTN。

ISDN BRI 端口：通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。

异步串口：主要应用于与 Modem 或 Modem 池的连接。

Console 端口：通过配置专用电缆连接至计算机串行口。

AUX 端口：在远程配置时使用。

答案：A

例 10-12　下面的 4 种路由中，哪一种路由的子网掩码是 255.255.255.255？__(23)__(2015 年下半年真题 23)

A. 远程网络路由　　B. 主机路由

C. 默认路由　　D. 静态路由

解析：因特网所有的分组转发都是基于目的主机所在的网络，但在大多数情况下都允许有这样的特例，即对特定的目的主机指明一个路由。这种路由就叫作特定主机路由。

答案：B

10.3.3　同步练习

1.　思科路由器的内存体系由多种存储设备组成，其中用来存放 IOS 引导程序的是__(1)__，运行时活动配置文件存放在__(2)__中。

(1)、(2)　A. FLASH　　B. ROM　　C. NVRAM　　D. DRAM

2. 路由器连接帧中继网络的接口是__(1)__，连接双绞线以太网的接口是__(2)__。

(1)、(2) A. AUI 接口 B. RJ-45 接口 C. Console 接口 D. Serial 接口

3. 在路由器配置过程中，要查看用户输入的最后几条命令，应该输入______。

A. show version B. show commands

C. show previous D. show history

10.3.4 同步练习参考答案

1. (1) A (2) C 2. (1) D (2) B 3. D

10.4 配置路由协议

10.4.1 考点辅导

10.4.1.1 配置 RIP 协议及其与 BFD 联动

1. 配置 RIP 协议

RIP 是距离矢量路由选择协议的一种。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时，路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器。这样，正确的路由信息逐渐扩散到全网。

RIP 使用非常广泛，它简单、可靠，便于配置。RIP 版本 2 还支持无类域间路由(ClasslessInter-Domain Routing，CIDR)、可变长子网掩码(Variable Length Subnetwork Mask, VLSM)和不连续的子网，并且使用组播地址发送路由信息。但是 RIP 只适用于小型的同构网络，因为允许的最大跳数为 15，任何超过 15 个站点的目的地均被标记为不可达。RIP 每隔 30s 广播一次路由信息。

RIP 应用于 OSI 网络七层模型的应用层。各厂家定义的管理距离(AD，即优先级)略有不同，华为定义的优先级是 100。

假设有如图 10-7 所示的网络拓扑结构，试通过配置使 RouterA、RouterB、RouterC 和 RouterD 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。

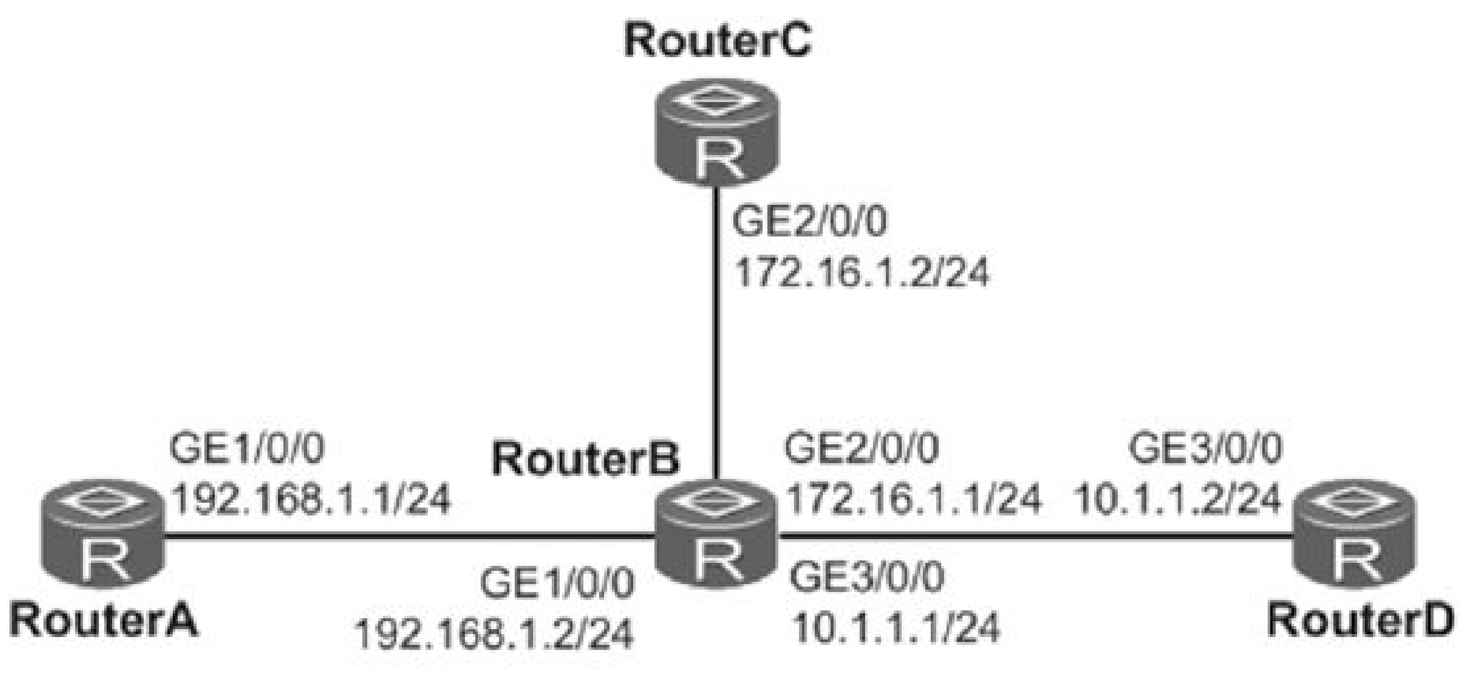


图 10-7 网络拓扑结构

1)　配置思路

采用如下的思路配置 RIP 的版本：

- 配置各接口的 IP 地址，使网络可达。
- 在各路由器上使能 RIP，配置 RIP 基本功能。
- 在各路由器上配置 RIP-2 版本，查看精确的子网掩码信息。

2)　数据准备

为完成此配置例，需准备如下的数据：

- 在 RouterA 上指定使能 RIP 的网段 192.168.1.0。
- 在 RouterB 上指定使能 RIP 的网段 192.168.1.0，172.16.0.0，10.0.0.0。
- 在 RouterC 上指定使能 RIP 的网段 172.16.0.0。
- 在 RouterD 上指定使能 RIP 的网段 10.0.0.0。
- 在 RouterA、RouterB、RouterC 和 RouterD 上配置 RIP-2 版本。

3)　操作步骤

(1)　配置各接口的 IP 地址(略)。

(2)　配置 RIP 基本功能。

①　配置 RouterA。

```
[RouterA] rip
[RouterA-rip-1] network 192.168.1.0
[RouterA-rip-1] quit
```

②　配置 RouterB。

```
[RouterB] rip
[RouterB-rip-1] network 192.168.1.0
[RouterB-rip-1] network 172.16.0.0
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] quit
```

③　配置 RouterC。

```
[RouterC] rip
[RouterC-rip-1] network 172.16.0.0
[RouterC-rip-1] quit
```

④　配置 RouterD。

```
[RouterD] rip
[RouterD-rip-1] network 10.0.0.0
[RouterD-rip-1] quit
```

⑤　查看 RouterA 的 RIP 路由表。

```
[RouterA] display rip 1 route
    Route Flags: R - RIP
            A - Aging, S - Suppressed, G - Garbage-collect
-------------------------------------------------------------------------
 Peer 192.168.1.2  on GigabitEthernet1/0/0
```

```
     Destination/Mask        Nexthop      Cost   Tag     Flags   Sec
        10.0.0.0/8          192.168.1.2     1     0        RA     14
        172.16.0.0/16       192.168.1.2     1     0        RA     14
```

从路由表中可以看出，RIP-1 发布的路由信息使用的是自然掩码。

(3) 配置 RIP 的版本。

① 在 RouterA 上配置 RIP-2。

```
[RouterA] rip
[RouterA-rip-1] version 2
[RouterA-rip-1] quit
```

② 在 RouterB 上配置 RIP-2。

```
[RouterB] rip
[RouterB-rip-1] version 2
[RouterB-rip-1] quit
```

③ 在 RouterC 上配置 RIP-2。

```
[RouterC] rip
[RouterC-rip-1] version 2
[RouterC-rip-1] quit
```

④ 在 RouterD 上配置 RIP-2。

```
[RouterD] rip
[RouterD-rip-1] version 2
[RouterD-rip-1] quit
```

(4) 验证配置结果。

查看 RouterA 的 RIP 路由表。

```
[RouterA] display rip 1 route
    Route Flags: R - RIP
             A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------------------
 Peer 192.168.1.2  on GigabitEthernet1/0/0
     Destination/Mask        Nexthop      Cost   Tag     Flags   Sec
        10.1.1.0/24         192.168.1.2     1     0        RA     32
        172.16.1.0/24       192.168.1.2     1     0        RA     32
```

从路由表中可以看出，RIP-2 发布的路由中带有更为精确的子网掩码信息。

2. RIP 与 BFD 联动

双向转发检测 BFD (Bidirectional Forwarding Detection)是一种用于检测邻居路由器之间链路故障的检测机制，它通常与路由协议联动，通过快速感知链路故障并通告使得路由协议能够快速地重新收敛，从而减少由于拓扑变化导致的流量丢失。

假设有如图 10-8 所示的网络拓扑结构，Router A、Router B 通过二层交换机 switch 互连，在设备上运行 RIP 协议来建立路由，同时使能允许 RIP 在双方接口上关联 BFD 应用。在 Router B 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告 RIP

协议，触发协议快速收敛。

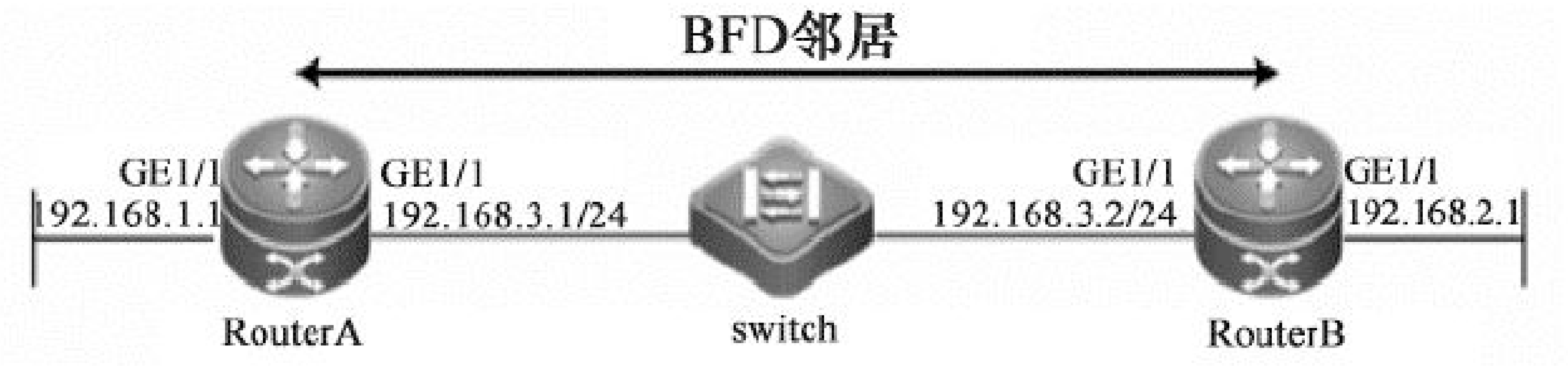


图 10-8 网络拓扑结构

1) Router A 的配置

(1) 配置 RIP 路由。

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#ip ref
RSR-A(config-GigabitEthernet 2/1)#ip address 192.168.3.1 255.255.255.0
RSR-A(config)#interface gigabitEthernet 1/1

RSR-A(config-GigabitEthernet 1/1)#ip ref
RSR-A(config-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
RSR-A(config-router)#  router rip
RSR-A(config-router)#  version 2
RSR-A(config-router)#  network 192.168.3.0
RSR-A(config-router)#  network 192.168.1.0
```

(2) 配置 RIP 与 BFD 联动。

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
//配置 BFD 时间参数，该命令同时启用了接口的 BFD 功能，因此必须配置；
//这里的 500/500/3 为推荐配置，间隔 500ms 发送一个探测报文，连续 3 个没收到回应宣告链路失败
RSR-A(config-GigabitEthernet 2/1)#no bfd echo
//推荐配置为该模式(ctrl 模式)，默认是 bfd echo 模式；和友商对接更是推荐 ctrl 模式，否则可能对接不起来
RSR-A(config-GigabitEthernet 2/1)#ip rip bfd
//在对应的接口开启 RIP 与 BFD 联动功能
```

2) Router B 的配置

(1) 配置 RIP 路由。

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#ip ref
RSR-B(config-GigabitEthernet 2/1)#ip address 192.168.3.2 255.255.255.0
RSR-B(config)#interface gigabitEthernet 1/1
RSR-B(config-GigabitEthernet 1/1)#ip ref
RSR-B(config-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
RSR-B(config-router)#  router rip
RSR-B(config-router)#  version 2
RSR-B(config-router)#  network 192.168.3.0
RSR-B(config-router)#  network 192.168.2.0
```

(2) 配置 RIP 与 BFD 联动。

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
RSR-B(config-GigabitEthernet 2/1)#no bfd echo
RSR-B(config-GigabitEthernet 2/1)#ip rip bfd
```

10.4.1.2 配置 IS-IS 协议

中间系统到中间系统 IS-IS(Intermediate System to Intermediate System)属于内部网关协议 IGP (Interior Gateway Protocol)，用于自治系统内部。为了支持大规模的路由网络，IS-IS 在自治系统内采用骨干区域与非骨干区域两级的分层结构。一般来说，将 Level-1 路由器部署在非骨干区域，Level-2 路由器和 Level-1-2 路由器部署在骨干区域。每一个非骨干区域都通过 Level-1-2 路由器与骨干区域相连。

IS-IS 是一种链路状态路由协议，每一台路由器都会生成一个 LSP，它包含了该路由器所有启用 IS-IS 协议接口的链路状态信息。通过跟相邻设备建立 IS-IS 邻接关系，互相更新本地设备的 LSDB，可以使得 LSDB 与整个 IS-IS 网络的其他设备的 LSDB 实现同步。然后根据 LSDB 运用 SPF 算法计算出 IS-IS 路由。如果此 IS-IS 路由是到目的地址的最优路由，则此路由会下发到 IP 路由表中，并指导报文的转发。

其相关命令如表 10-1 所示。

表 10-1 IS-IS 的相关命令及功能

命 令	功 能
isis [process-id]	创建 IS-IS 进程并进入 IS-IS 视图
Isis circuit-level[level-1|level-1-2|level-2]	设置接口的 Level 级别，默认情况下，接口的 Level 级别为 level-1-2
Network-entity net	设置网络实体名称
Net	格式为 x…x.xxxx.xxxx.xxxx.00，前面的“x…x”是区域地址，中间的 12 个“x”是路由器的 System ID，最后的“00”是 SEL
Isis enable[process-id]	指定 IS-IS 的进程号，默认为 1，IS-IS 将通过该接口建立邻居、扩散 LSP 报文
Display isis peer	查看 IS-IS 的邻居信息
Display isis route	查看 IS-IS 的路由信息

10.4.1.3 配置 OSPF 协议

开放最短路径优先协议是重要的路由选择协议，它是一种链路状态路由选择协议，是由 Internet 工程任务组开发的内部网关路由协议，用于在单一自治系统内决策路由。

链路是路由器接口的另一种说法，因此，OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。下面分别介绍 OSPF 协议的相关要点。

(1) 自治系统。自治系统包括一个单独管理实体下所控制的一组路由器，OSPF 是内部网关路由协议，工作于自治系统内部。

(2) 链路状态。所谓链路状态，是指路由器接口的状态，例如 Up. Down、IP 地址、网

络类型、链路开销以及路由器和它邻接路由器间的关系。链路状态信息通过链路状态通告(Link State Advertisement，LSA)扩散到网络上的每台路由器，每台路由器根据 LSA 信息建立一个关于网络的拓扑数据库。

(3) 最短路径优先算法。OSPF 协议使用最短路径优先算法，利用从 LSA 通告得来的信息计算到达每一个目标网络的最短路径，以自身为根生成一棵树，包含了到达每个目的网络的完整路径。

(4) 路由器标识。OSPF 的路由标识是一个 32 位的数字，它在自治系统中被用来唯一地识别路由器。默认使用最高回送地址，若回送地址没有被配置，则使用物理接口上最高的 IP 地址作为路由器标识。

(5) 邻接和邻居。OSPF 在相邻路由器间建立邻接关系，使它们交换路由信息。邻居是指共享同一网络的路由器，并使用 Hello 包来建立和维护邻居路由器间的邻接关系。

(6) 区域。在 OSPF 网络中使用区域(Area)为自治系统分段。OSPF 是一种层次化的路由选择协议，区域 0 是一个 OSPF 网络中必须具有的区域，也称为主干区域，其他所有区域要求通过区域 0 互连到一起。

其相关命令及说明如表 10-2 所示。

表 10-2 OSPF 的相关命令及功能

命 令	功 能
ospf[process-id|router-id router-id|vpn-instance vpn-instance-name]	启动 OSPF 进程，进入 OSPF 视图
area area-id	创建并进入 OSPF 区域视图
network ip-address wildcard-mask	配置区域所包含的网段
display ospf peer	查看 OSPF 邻居信息
display ospf routing	查看 OSPF 路由信息

10.4.1.4 配置 BGP 协议

边界网关协议 BGP(Border Gateway Protocol)是一种实现自治系统 AS (Autonomous System)之间的路由可达，并选择最佳路由的距离矢量路由协议。它具有以下特点。

(1) 实现自治系统间通信网络的信息可达。BGP 允许一个 AS 向其他 AS 通告其内部网络的可达性信息，或者是通过该 AS 可达的其他网络的路由信息。

(2) 多个 BGP 路由器之间的协调。如果在一个自治系统内部有多个路由器分别使用 BGP 与其他自治系统中对等路由器进行通信，则通过协调使这些路由器保持路由信息的一致性。

(3) BGP 支持基于策略的路径选择。可以为域内和域间的网络可达性配置不同的策略。

(4) BGP 只需要在启动时交换一次完整信息。不需要在所有路由更新报文中传送完整的路由数据库信息，后续的路由更新报文只通告网络的变化信息，避免网络变化使得信息量大幅增加。

(5) 在 BGP 通告目的网络的可达性信息时。除了处理指定目的网络的下一跳信息之外，通告中还包括了通路向量，即去往该目的网络时需要经过的 AS 的列表，使接受者能够清楚了解去往目的网络的通路信息。

除了以上这些，BGP 允许发送方把路由信息聚集在一起，用一个条目来表示多个相关的目的网络，以节约网络带宽。允许接收方对报文进行鉴别，以验证发送方的身份等多个特点。

BGP 在不同自治系统(AS)之间进行路由转发，分为 EBGP 和 IBGP 两种情况。EBGP 外部边界网关协议，用于在不同的自治系统间交换路由信息。IBGP 内部边界网关协议，用于向内部路由器提供更多信息。

其相关命令及说明如表 10-3 所示。

表 10-3　BGP 的相关命令及功能

命　令	功　能
bgp{as—number-plain|as-number-dot}	启动 BGP，指定本地 AS 编号，并进入 BGP 视图
router-id ipv4-address	配置 BGP 的 Router ID
peer{ipv4-address|ipv6-address}as-number{as-number-plain|as-number-dot}	创建 BGP 对等体
ipv4-family {unicast|multicast}	进入 IPv4 地址族视图
import-route direct	管理 IP 所在的网段路由，并引入 RIP 路由表

10.4.2　典型例题分析

例 10-13　运行 OSPF 协议的路由器在选举 DR/BDR 之前，DR 是__(58)__。(2017 年上半年真题 58)

A. 路由器自身　　B. 直连路由器

C. IP 地址最大的路由器　　D. MAC 地址最大的路由器

解析：在运行 OSPF 路由协议的广播多路型网络中，初始阶段 OSPF 路由器会在 hello 包中将 DR 和 BDR 指定为 0.0.0.0，当路由器收到邻居的 hello 包时，就会检查 hello 包中携带的路由器优先级、DR 和 BDR 等字段，然后列举出具备 DR 和 BDR 资格的路由器。

答案：A

例 10-14　关于 OSPF 路由协议的说法中，正确的是__(59)__。(2017 年上半年真题 59)

A. OSPF 路由协议是一种距离矢量路由协议

B. OSPF 路由协议中的进程号全局有效

C. OSPF 路由协议不同进程之间可以进行路由重分布

D. OSPF 路由协议的主区域为区域

解析：OSPF(Open Shortest Path First，开放式最短路径优先)是一个内部网关协议(Interior Gateway Protocol，简称 IGP)，用于在单一自治系统(Autonomous System，AS)内决策路由，是对链路状态路由协议的一种实现，隶属内部网关协议(IGP)，故运作于自治系统内部。其进程号只具备本地意义。其主干区域号为 0，不同的 OSPF 进程可以进行重发布。

答案：C

例 10-15　下面的提示符__(56)__表示特权模式。(2016 年下半年真题 56)

A. >　　B. #　　C. (config)#　　D. !

解析：用户模式>:在 Cisco 设备启动工作完成之后，即进入用户模式。在用户模式下，只允许基本的监测命令，比如 ping 其他网络设备，在这种情况下不能改变路由器的配置。

特权模式#：在用户模式下输入 enable 命令，进入特权模式。在特权模式下，可以使用 show 命令来观察设备的状况和我们所做的配置。在特权模式下不能对设备进行配置。

全局模式(config)#：在特权模式下输入 config terminal 命令，即可进入全局模式。在全局模式下可以对网络设备进行配置，并且在全局模式下所做的配置对整个设备都有效。

如果需要对某个接口进行单独的配置，就需要从全局模式进入这个接口子模式。

答案：B

例 10-16　把路由器当前配置文件存储到 NVRAM 中的命令是__(57)__。(2016 年下半年真题 57)

A. Router(config)#copy current to starting

B. Router#copy starting to running

C. Router(config)#copy running-config starting-config

D. Router#copy run startup

解析：把路由器当前配置文件存储到 NVRAM 中的命令可以用 Router#copy run startup。D 选项为缩写，实际上是 copy running-config startup-config，该命令需在特权模式下配置。

答案：D

例 10-17　如果要将目标网络为 202.117.112.0/24 的分组经 102.217.115.1 接口发出，需增加一条静态路由，正确的命令是__(30)__。(2015 年下半年真题 30)

A. Route add 202.117.112.0 255.255.255.0 102.217.115.1

B. Route add 202.117.112.0 0.0.0.255 102.217.115.1

C. add route 202.117.112.0 255.255.255.0 102.217.115.1

D. add route 202.117.112.0 0.0.0.255 102.217.115.1

解析：添加静态路由的格式是：

```
route add [-net|-host] [网络或主机] netmask [mask] [gw|dev]
```

答案：A

例 10-18　配置路由器接口的提示符是__(57)__。(2015 年下半年真题 57)

A. router (config)#　　　　B. router (config-in)#

C. router (config-intf)#　　　　D. router (config-if) #

解析：路由器的基本配置如下。

(1)　进入特权模式。

```
Router>                (用户模式提示符)
Router> enable         (进入特权模式)
Password:<password>    (输入口令)
Router #               (特权模式提示符)
```

(2)　进入全局配置模式。

```
Router # ip routing            (启动路由协议)
Router # config terminal       (输入 config termial 命令进入配置模式)
Router(config)#                (配置模式提示符)
```

(3) 配置接口。

```
Router(config)# interface fastethernet0/1        (进入接口 F0/1 子配置模式)
Router(config-if)# ip address 192.168.0.1 255.255.255.0
(设置该接口的 IP 地址，格式为：ip address ip-addr subnet-mask)
Router(config-if)# no shutdown                   (激活接口)
Router(config-if)# exit                          (返回至全局配置模式)
```

如果有多个接口需配置，则重复步骤(3)。

(4) 查看配置，保存配置。

```
Router(config)# end                    (退回到特权模式)
Router # Show running-config           (查看配置)
Router # write                         (保存配置)
```

答案：D

例 10-19 如果想知道配置了哪种路由协议，应使用的命令是__(58)__。(2015 年下半年真题 58)

A. router>show router protocol　　B. Router (config)>show ip protocol

C. router (config)>#show router protocol　　D. router >show ip protocol

解析：show 命令可以同时在用户模式和特权模式下运行，“show ？”命令用来提供一个可利用的 show 命令列表。show ip protocol 用来查看当前路由器运行的动态路由协议情况。

答案：D

例 10-20 如果在互联网中添加了一个局域网，要用手工方式将该局域网添加到路由表中，应使用的命令是__(59)__。(2015 年下半年真题 59)

A. router(config)>ip route 2.0.0.0 255.0.0.0 via 1.0.0.2

B. router(config)#ip route 2.0.0.0 255.0.0.0 1.0.0.2

C. router (config) #ip route 2.0.0.0 via 1.0.0.2

D. router (config) #ip route 2.0.0.0 1.0.0.2 mask 255.0.0.0

解析：

router(config)# ip route network [mask] {address|interface} [distance] [permanent]:

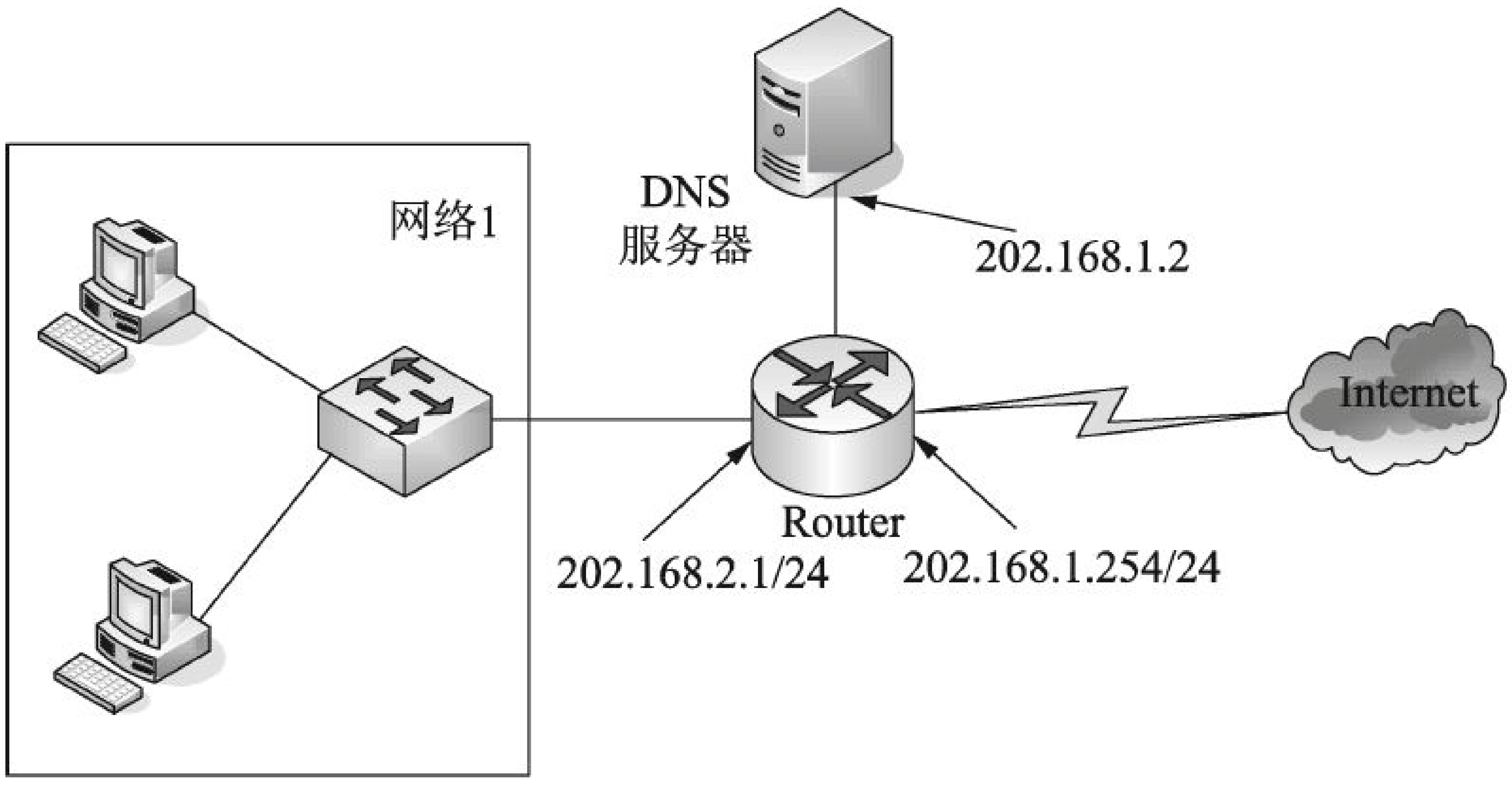
[distance] [permanent]是配置浮动静态路由的选项，在软考中不会考查。浮动静态路由是一种特殊的静态路由，通过配置一个比主路由的管理距离更大的静态路由，保证网络中主路由失效的情况下，提供备份路由。但在主路由存在的情况下它不会出现在路由表中。

{address|interface}，在静态地添加到达目的网络的路由的时候，可以指定路径中下一台设备的地址，也可以指定与下一台设备连接的自己这台路由器的接口。

答案：B

10.4.3 同步练习

网络配置如下图所示，在路由器 Router 中配置网络 1 访问 DNS 服务器的主机路由的命令是__(1)__。网络 1 访问 Internet 的默认路由命令是__(2)__。



(1)、(2)　A. ip route 202.168.1.2 255.255.255.0 202.168.1.2
B. ip route 202.168.1.2 255.255.255.255 202.168.1.2
C. ip route 0.0.0.0 0.0.0.0 202.168.1.253
D. ip route 255.255.255.255 0.0.0.0 202.168.1.254

10.4.4　同步练习参考答案

(1) B　(2) C

10.5　配置广域网接入

10.5.1　考点辅导

如果要将网络与其他远程网络连接起来，有时要用到广域网(NVAN)接入服务。本节结合具体的 PPP、帧中继 FR 和 ISDN BRI 连接接入实例来学习广域网接入的配置方法和技巧。

10.5.1.1　配置 PPP 和 DCC

点对点协议是作为在点对点链路上进行 IP 通信的封装协议而被开发出来的。PPP 定义了 IP 地址的分配和管理、异步和面向位的同步封装、网络协议复用、链路配置、链路质量测试和错误检测等标准，以及网络层地址协议和数据压缩协议等协议标准。PPP 通过可扩展的链路协议和网络控制协议(NCP)来实现上述功能。

PPP 具有多协议支持的特点，可以支持 IP、IPX 和 DECnet 等第三层协议。PPP 提供了安全认证机制，这主要是通过 PAP(口令认证协议)和 CHAP(挑战握手协议)来实现的。PAP 和 CHAP 被用来认证是否允许对端设备进行拨号连接。

多链路 PPP 是 PPP 的另一项功能，它允许在路由器和路由器之间或路由器和拨号的 PC 之间建立多条链路，通信量在这些链路之间进行负载均衡，从而提高了可用带宽和链路的可靠性。

按需拨号路由(Dial Control Center，DCC)是利用拨号链路实现网络间互联的一种常用技术。其主要功能是将数据包从被拨号的接口进行路由；决定何种数据包可以触发拨号；决

定什么时候终止连接。DCC 技术和 PPP 技术一样对于 ISDN 的配置是非常重要的，在实际应用中 ISDN、PPP 和 DCC 这三项技术经常综合使用。

相关命令及说明如表 10-4 所示。

表 10-4　PPP 的相关配置命令

命　令	功　能
interface mp-group	创建 MP-Group 接口并进入 MP-Group 接口视图
local-user user-name password	创建本地账号，并配置本地账号的登录密码
local-user user-name service-type ppp	配置本地用户使用的服务类型为 PPP
ppp authentication-mode{chap|pap}[[call-in]domain domain-name]	配置本端设备对端设备的认证方式
authentication-scheme scheme-name	建立认证方案
domain domain-name	配置默认域
ppp chap user username	配置采用 CHAP 认证时认证方的用户名
ppp mp mp-group number	物理接口加入指定的组

10.5.1.2　配置帧中继

帧中继是一种高性能的 WAN 协议，运行在 OSI 参考模型的物理层和数据链路层。它是一种数据包交换技术，是 X.25 的简化版本。它省略了 X.25 的一些强健功能，如提供窗口技术和数据重发技术，而是依靠高层协议提供纠错功能，这是因为帧中继工作在更好的 WAN 设备上，这些设备较之 X.25 的 WAN 设备具有更可靠的连接服务和更高的可靠性，它严格地对应于 OSI 参考模型的最低两层，而 X. 25 还提供第三层的服务，所以帧中继比 X.25 具有更高的性能和更有效的传输效率。

帧中继广域网的设备分为 DTE 和 DCE。DTE 表示数据终端设备，DCE 表示数据通信设备，用于将用户 DTE 设备接入网络。

帧中继技术提供面向连接的数据链路层通信，在每对设备之间都存在一条定义好的通信链路，且该链路有一个链路识别码。这种服务通过帧中继虚电路实现，每个帧中继虚电路都以数据链路识别码(DLCI)标识自己。DLCI 的值一般由帧中继服务提供商指定。帧中继既支持 PVC 也支持 SVC。

其相关命令及说明如表 10-5 所示。

表 10-5　帧中继的相关配置命令

命　令	功　能
link-protocol fr	设置 Frame Relay 封装
fr interface-type dte	设置 Frame Relay 接口类型 DTE
fr dlci dlci	配置帧中继链路的数据连接标识符
fr map ip	配置本端 DLCI 到对端 IP 地址的静态映射

10.5.1.3　配置 ISDN

综合业务数字网(Integrated Service Digital Network，ISDN)是电话网络数字化的结果，

由数字电话和数据传输服务两部分组成，可以在 ISDN 上传输声音、数据和视频等多种信息。ISDN 组件包括终端、终端适配器、网络终端设备、线路终端设备和交换终端设备等。

ISDN 提供了两种类型的访问接口，即基本速率接口(Basic Rate Interface，BRI)和主要速率接口(Primary Rate Interface，PRI)。ISDN BRI 提供两个 B 信道和一个 D 信道(2B+D)。ISDN 的 B 信道为承载信道，其速率为 64kbps，用于传输用户数据；D 信道速率为 16kbps，主要用于传输控制信息。PRI 提供 30 个 B 信道和一个 D 信道(30B+D)，其 B 信道和 D 信道的速率均为 64kbps。

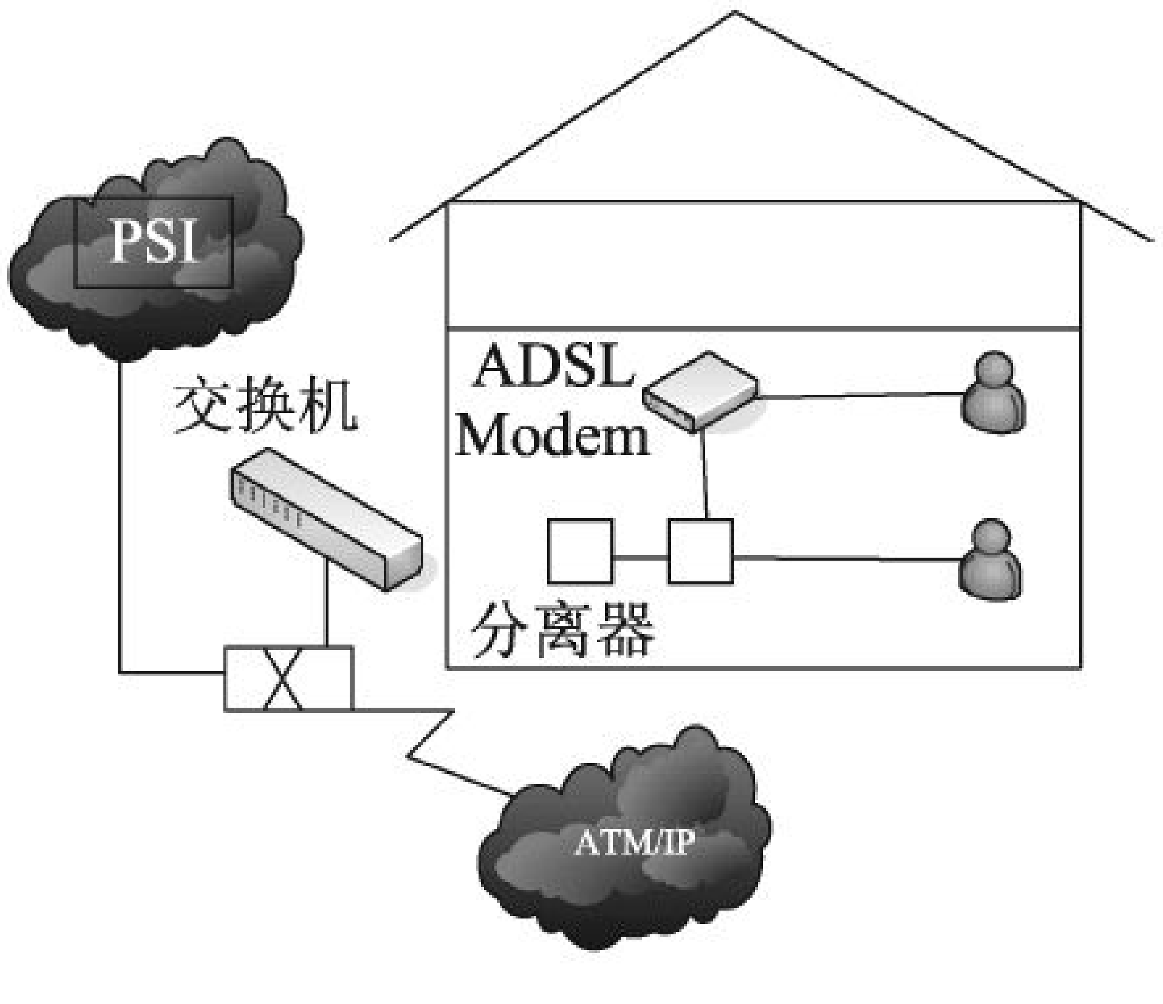
其相关命令及说明如表 10-6 所示。

表 10-6　ISDN 的相关配置命令

命　令	功　能
dialer-rule	进入 Dialer-rule 视图
dialer-rule dialer-rule-number {acl{acl-number|name acl-name}|ip{deny|permit}|ipv6{deny|permit}}	配置某个拨号访问组对应的拨号访问控制列表，指定引发 DCC 呼叫的条件
dialer enable-circular	使能轮询 DCC 功能
interface bri interface-number	进入指定的 ISDN BRI 接口
display isdn call-info [interface interface-type interface-number]	查看 ISDN 接口的当前呼叫状态
isdn statistics{clear|continue|display[flow]|start|stop}	ISDN 接口信息统计

10.5.2　典型例题分析

例 10-21　下图是家庭用户安装 ADSL 宽带网络时的拓扑结构，图中左下角的×是__(1)__设备；为了建立虚拟拨号线路，在用户终端上应安装__(2)__协议。



(1)　A. DSLAM　　B. Hub　　C. ADSL Modem　　D. IP Router

(2)　A. ARP　　B. HTTP　　C. PPTP　　D. PPPoE

解析：在 ISP 端通过接入多路复用器(DSL Access Multiplex，DSLAM)连接到因特网。PPPoE(Point-to-Point Protocol over Ethernet)可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入集中器上。通过 PPPoE，远端接入设备能够实现对每个接入用户的控制

和计费。

答案：(1) A (2) D

10.5.3 同步练习

点对点协议简称________。

A. PTP B. PPP C. DDR D. PAP

10.5.4 同步练习参考答案

B

10.6 IPSec 配置与测试

10.6.1 考点辅导

10.6.1.1 IPSec 实现的工作流程

IPSec 实现的 VPN 有多种方式，本节介绍通过 IKE 协商方式建立 IPSec 隧道的配置。IKE 动态协商方式是由 ACL 来指定要保护的数据流范围，配置安全策略并将安全策略绑定在实际的接口上来完成 IPSec 的配置。具体方法是通过 ACL 规则筛选出需要进入 IPSec 隧道的报文，规则允许(permit)的报文将被保护，规则拒绝(deny)的报文将不被保护。这种方式可以利用 ACL 配置的灵活性，根据 IP 地址、端口、协议类型等对报文进行过滤进而灵活制定安全策略，在中大型网络中，一般使用 IKE 协商建立 SA。

1. 为 IPSec 做准备

在采用 ACL 方式建立 IPSec 隧道之前，实现源接口和目的接口之间路由可达。如果要配置基于 ACL 的 GRE over IPSec，则需要创建一个 Tunnel 接口并配置该接口为 GRE 类型，配置源 IP、目的 IP 和 IP 地址。其中，源 IP 为网关出接口的 IP，目的 IP 为对端网关出接口的 IP 地址，并将 Tunnel 接口加入安全区域。

2. 定义需要保护的数据

IPSec 能够对一个或多个数据流进行安全保护，ACL 方式建立 IPSec 隧道采用 ACL 来指定需要 IPSec 保护的数据流。实际应用中，首先需要通过配置 ACL 的规则定义数据流范围，再在 IPSec 安全策略中引用该 ACL，从而起到保护该数据流的作用。一个 IPSec 安全策略中只能引用一个 ACL。

3. 配置 IPSec 安全提议

IPSec 安全提议是安全策略或者安全框架的一个组成部分，它包括 IPSec 使用的安全协议、认证/加密算法以及数据的封装模式，定义了 IPSec 的保护方法，为 IPSec 协商 SA 提供

各种安全参数。IPSec 隧道两端设备需要配置相同的安全参数。

4. 配置 IPSec 安全策略

IPSec 安全策略是创建 SA 的前提，它规定了对哪些数据流采用哪种保护方法。配置 IPSec 安全策略时，通过引用 ACL 和 IPSec 安全提议，将 ACL 定义的数据流和 IPSec 安全提议定义的保护方法关联起来，并可以指定 SA 的协商方式、IPSec 隧道的起点和终点、所需要的密钥和 SA 的生存周期等。一个 IPSec 安全策略由名称和序号共同唯一确定，相同名称的 IPSec 安全策为一个 IPSec 安全策略组。

5. 接口上应用 IPSec 安全策略组

为使接口能对数据流进行 IPSec 保护，需要在该接口上应用一个 IPSec 安全策略组。当取消 IPSec 安全策略组在接口上的应用后，此接口便不再具有 IPSec 的保护功能。IPSec 安全策略组是所有具有相同名称、不同序号的 IPSec 安全策略的集合。

6. 测试和验证 IPSec

该任务涉及使用 display ipsec global config、ping 和相关的命令来测试和验证 IPSec 加密工作是否正常，并为之排除故障。

10.6.1.2　常见的故障

1. IKE SA 协商失败

IPSec 业务不通时，执行命令 display ike sa，发现 IKE SA 没有协商成功。IKE SA 协商失败时，显示信息为空、Flag 参数为空或者 Peer 参数为 0.0.0.0。

排错方法 1：使用命令 display ike proposal，查看 IKE 对等体间的 IKE 安全提议是否一致，如果不一致需要配置一致。例如检查发现认证算法不一致。

IKE 协商的发起方：

```
ike proposal 10
authentication-algorithm sha2-256
```

IKE 协商的响应方：

```
ike proposal 10
authentication-algorithm sha2-384
```

排错方法 2：使用命令 display ike peer，查看对等体视图下的配置是否有遗漏或配置错误。检查是否配置对端 IP 地址。

采用 ACL 方式建立 IPSec 隧道时，如果 IKE 协商采用主模式，则设备必须指定对端的 IP 地址，而且两端指定的对端 IP 地址要相互匹配。

例如 IKE 协商的发起方和响应方的 IP 地址分别为 10.1.1.2 和 10.2.1.2，配置如下所示。

IKE 协商的发起方：

```
ike peer mypeer1
remote-address 10.2.1.2
```

IKE 协商的响应方：

```
ike peer mypeer2
remote-address 10. 1. 1.2
```

对端 outbound 的 spi 值与本端的 inbound 不同或配置的策略不同(esp、ah)。

判断方法和解决方案为：检查双方的配置信息，尤其是在 IPSec-manual 方式下检查双方的 SPI 值是否按方向(inbound、outbound)匹配。而在 IPSec-isakmp 下，则可能是协商出错。

2. IPSec SA 协商失败

问题描述：IPSec 业务不通时，执行命令 display ike sa，发现 IPSec SA 没有协商成功，第二阶段的显示信息未显示或 Flag 参数为空。

排错方法 1：执行命令 display ipsec proposal，查看 IKE 对等体间的 IPSec 安全提议是否一致，如果不一致需要配置一致。例如检查发现 ESP 协议采用的认证算法不一致。

IKE 协商的发起方：

```
ipsec proposal prop1
esp authentication-algorithm sha2-512
```

IKE 协商的响应方：

```
ipsec proposal prop2
esp authentication-algorithm sha2-384
```

排错方法 2：使用命令 display ipsec policy，查看 IPSec 安全策略视图下的配置是否有遗漏或配置错误。检查 IPSec 安全策略中引用的 ACL 是否一致。

当 IPSec 隧道两端的 ACL 规则镜像配置时，任意一方发起协商都能保证 SA 成功建立；当 IPSec 隧道两端的 ACL 规则非镜像配置时，只有发起方的 ACL 规则定义的范围是响应方的子集时，SA 才能成功建立。因此，建议 IPSec 隧道两端配置的 ACL 规则互为镜像，即一端配置的 ACL 规则的源地址和目的地址分别为另一端配置的 ACL 规则的目的地址和源地址。

例如 IKE 协商的发起方源/目的地址为 172.16.10.2/172.16.20.2，IKE 协商的响应方源/目的地址为 172.16.20.2/172.16.10.2。

IKE 协商的发起方：

```
acl number 3001
rule 5 permit ip source 172.16.10.0 0.0.0.255 destination 172.16.20.00.
0.0.255
ipsec policy map1 10 isakmp
security acl 3001
```

IKE 协商的响应方：

```
acl number 3001
rule 5 permit ip source  172.16.20.0 0.0.0.255 destination 172.16.10.0 0.0.0.255
ipsec policy map2 10 isakmp
security acl 3001
```

检查 IPSec 安全策略中引用的 IKE 对等体中内容是否一致，如果不一致需要配置一致。例如 IKE 协商的发起方引用的 IKE 对等体为 spub。

```
ipsec policy map1 10 isakmp
ike-peer spub
```

其 IKE 对等体的相关配置为：

```
ike peer spub
undo version 2
pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7'DEV&=G(=Et02P/%\*!%^%#
//密钥#JHuawei@123
ike-proposal 5
remote-address 59.74.144.1
```

检查 IPSec 安全策略中引用的 IPSec 安全提议中内容是否一致，如果不一致需要配置一致。例如 IKE 协商的发起方引用的 IPSec 安全提议为 tran1。

```
ipsec policy policy1 100 isakmp
proposal tran1
```

IPSec 安全提议的相关配置为：

```
ipsec proposal tran1
esp authentication-algorithm sha2-256
esp encryption-algorithm aes-128
```

10.6.1.3　测试时常见的故障

1. 故障 1

问题描述：在 IPSec-manual 或 IPSec-isakmp 方式下，双方配置好后或双方协商通过后，仍然无法相互通信。同时若打开 debug crypto packet，则会出现以下信息：

```
rec'd IPSEC packet from IPADDR has invalid spi
```

原因：对端的 outbound 的 spi 值与本端的 inbound 不同或配置的配置策略不同(esp、ah)。

判断方法和解决方案：检查双方的配置信息，尤其是在 IPSec-manual 方式下，检查双方的 SPI 值是否按方向(inbound、outbound)匹配。而在 IPSec-isakmp 方式下，则可能是协商出错。

2. 故障 2

问题描述：在 IPSec-manual 方式下，双方配置好后，仍然无法相互通信。同时若打开 debug crypto packet，则会出现以下信息：

```
packet missing policy
```

原因：对端的 outbound 的配置策略和本地不同(esp、ah)。

判断方法和解决方案：检查双方的配置信息，很可能是对端策略配置为 esp，而本端策略为 ah+esp。

3. 故障 3

问题描述：在 IPSec-manual 方式下，双方配置好后，仍然无法相互通信。同时若打开

debug crypto packet，则会出现以下信息：

```
rec'd IPSEC packet from IPADDR has bad padding.
```

原因：对端的 outbound 的加密密钥与本端的 inbound 的不同。

判断方法和解决方案：检查对端的 outbound 的加密密钥和本端的 inbound 的加密密钥，务必使两者相同。

4. 故障 4

问题描述：在 IPSec-manual 方式下，双方配置好后，仍然无法相互通信。同时若打开 debug crypto packet，则会出现以下信息：

```
rec'd IPSEC packet mac verify failed.
```

原因：对端的 outbound 的 ESP 或 AH 验证密钥与本端的 inbound 的不同。

判断方法和解决方案：检查对端的 outbound 的 ESP 或 AH 验证密钥和本端的 inbound 的验证密钥，务必使两者相同。

5. 故障 5

问题描述：在 IPSec-manual 方式下，双方配置好后，仍然无法相互通信。同时若打开 debug crypto packet，则会出现以下信息：

```
rec'd IPSEC packet from IPADDR to IPADDR does not agree with policy.
```

原因：IPSec 处理完成的包与相应的 access-list 不同，子 MAP 的访问列表配置有问题。

判断方法和解决方案：检查本端 sub_map 配置的 access-list 是否符合进行 IPSec 通信的要求。

6. 故障 6

问题描述：在 IPSec-isakmp 方式下，双方配置好后，由对端开始发起协商，无法进行通信，show crypto isakmp sa 也没有发现和当前通信相关的成功的 SA 信息。在协商的同时若打开 debug crypto isakmp，则会出现以下信息：

```
ISAKMP(xxx): processing ISAKMP-SA payload(随后有若干 transform-payload 中的
内容)ISAKMP(xxx):no acceptable Oakley Transform ISAKMP(xxx): negotiate error
NO_PROPOSAL_CHOSEN.
```

原因：双方配置的 ISAKMP 策略不匹配。

判断方法和解决方案：检查两端的 ISAKMP.Policy 是否相同，尤其是对端的 lifetime 值不能大于本地的 lifetime 值。

7. 故障 7

问题描述：在 IPSec-isakmp 方式下，双方配置好后，由对端开始发起协商，无法进行通信，show crypto ipsec sa 也没有发现和当前通信相关的成功的 SA 信息。在协商的同时若打开 debug crypto isakmp，则会出现以下信息：

```
ISAKMP(xxx): processing IPSec-SA payload(随后有若干 transform-payload 中的内
容)ISAKMP(xxx): no acceptable Proposal in IPsec SA ISAKMP(xxx): negotiate
error NO_PROPOSAL_CHOSEN.
```

原因：双方配置的 IPSec 策略不匹配。

判断方法和解决方案：检查两端的相应的 transform-set 是否匹配，相应的 sub_map 下的 pfs 属性是否相同。

8. 故障 8

问题描述：在 IPSec-isakmp 方式下，双方配置好后，由对端开始发起协商，无法进行通信，show crypto ipsec sa 也没有发现和当前通信相关的成功的 SA 信息。在协商的同时若打开 debug crypto isakmp，则会出现以下信息：

```
ISAKMP: attr accept again transform-set xxx... ISAKMP(xxx): dealing with
ID-payload(随后有对端为 IPSec 通信所配置的 access-list 内容)ISAKMP(xxx):ISAKMP:
not found matchable policy.
```

原因：双方配置的 IPSec 规则不匹配。

判断方法和解决方案：检查两端相应的 sub_map 下的规则(access-list)是否匹配。

9. 故障 9

问题描述：在 IPSec-isakmp 方式下，双方配置好后，由本端开始发起协商，无法进行通信，show crypto isakmp sa 也没有发现和当前通信相关的成功的 SA 信息。在协商的同时若打开 debug crypto isakmp，则会出现以下信息：

```
ISAKMP(xxx): dealing with Notify Payload ISAKMP:
Notify-Message: NO_PROPOSAL_CHOSEN.
```

原因：双方配置的 ISAKMP 策略不匹配。

判断方法和解决方案：检查两端的 ISAKMP-Policy 是否匹配。

10. 故障 10

问题描述：在 IPSec-isakmp 方式下，双方配置好后，由本端开始发起协商，无法进行通信，show crypto isakmp sa 发现和当前通信相关的成功(M_SA_SETUP)的 SA 信息，但是 show crypto ipsec sa 无相关的 SA 信息。在协商的同时若打开 debug crypto isakmp，则会出现以下信息：

```
ISAKMP(xxx): dealing with Notify Payload ISAKMP: Notify-Message:
NO_PROPOSAL_CHOSEN.
```

原因：双方配置的 IPSec 策略不匹配，或配置的规则(access-list)不匹配。

判断方法和解决方案：检查两端的相应的 transform-set 是否匹配，相应的 sub_map 下的 pfs 属性和规则(access-list)是否匹配。

11. 故障 11

问题描述：在 IPSec-isakmp 方式下，双方配置好后，由一方开始发起协商，无法进行通信，show crypto ipsec sa 无相关的 SA 信息。在协商的同时若打开 debug crypto isakmp，

则会出现以下信息：

```
ISAKMP(xxx): dealing with Notify Payload ISAKMP: Notify-Message:
INVALID-EXCHANGE-TYPE 或 ISAKMP(xxx): negotiate error
INVALID-EXCHANGE-TYPE.
```

原因：对端不支持此种类型的协商报文。

判断方法和解决方案：改变对端设置，更换一种模式(比如由 Aggressive 模式换成 Main 模式)。

10.6.2 典型例题分析

例 10-22 在 IPSec-manual 或 IPSec-isakmp 方式下，双方配置好后或双方协商通过后，仍然无法相互通信。同时若打开 debug crypto packet，则会出现以下信息：

```
rec'd IPSEC packet from IPADDR has invalid spi.
```

出现此故障的原因是________。

A. 对端的 outbound 的 spi 值与本端的 inbound 不同或配置的配置策略不同(esp、ah)

B. 对端的 outbound 的配置策略和本地不同(esp、ah)

C. 对端的 outbound 的加密密钥与本端的 inbound 不同

D. 对端的 outbound 的 ESP 或 AH 验证密钥与本端的 inbound 不同

解析：判断方法和解决方案：检查双方的配置信息，尤其是在 IPSec-manual 方式下，检查双方的 SPI 值是否按方向(inbound、outbound)匹配。在 IPSec-isakmp 方式下，则可能是协商出错。

答案：A

10.6.3 同步练习

1. 在 IPSec-manual 方式下，双方配置好后，仍然无法相互通信。同时若打开 debug crypto packet，则会出现以下信息：

```
rec'd IPSEC packet from IPADDR to IPADDR does not agree with policy.
```

出现此故障的原因是________。

A. IPSec 处理完成的包与相应的 access-list 不同，子 MAP 的访问列表配置有问题

B. 双方配置的 ISAKMP 策略不匹配

C. 双方配置的 IPSec 策略不匹配

D. 双方配置的 IPSec 规则不匹配

2. 某客户端采用 ping 命令检测网络连接故障时，发现可以 ping 通 127.0.0.1 及本机的 IP 地址，但无法 ping 通同一网段内其他工作正常的计算机的 IP 地址。该客户端的故障可能是______。

A. TCP/IP 不能正常工作　　B. 本机网卡不能正常工作

C. 本机网络接口故障　　D. 本机 DNS 服务器地址设置错误

10.6.4　同步练习参考答案

1. A　　2. C

10.7　IPv6 配置与部署

考点辅导

1. IPv6-over-IPv4 GRE 隧道配置

IPv6-over-IPv4 隧道是将 IPv6 报文封装在 IPv4 报文中，让 IPv6 数据包穿过 IPv4 网络进行通信。对于采用隧道技术的设备来说，在隧道的入口处，将 IPv6 的数据报封装进 IPv4，IPv4 报文的源地址和目的地址分别是隧道入口和隧道出口的 IPv4 地址：在隧道的出口处，再将 IPv6 报文取出转发到目的节点。隧道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，容易实现。但是，隧道技术不能实现 IPv4 主机与 IPv6 主机的直接通信。

使用标准的 GRE 隧道技术，可以在 IPv4 的 GRE 隧道上承载 IPv6 数据报文。GRE 隧道是两点之间的连路，每条连路都是一条单独的隧道。GRE 隧道把 IPv6 作为乘客协议，将 GRE 作为承载协议。所配置的 IPv6 地址是在 Tunnel 接口上配置的，所配置的 IPv4 地址是 Tunnel 的源地址和目的地址(隧道的起点和终点)。

IPv6-over-IPv4GRE 隧道的相关配置命令及功能如表 10-7 所示。

表 10-7　GRE 隧道的相关配置命令及功能

命　令	功　能
interface tunnel interface-number	创建 Tunnel 接口
tunnel-protocol gre	指定 Tunnel 为 GRE 模式
source {ip-address | interface-type interface-number}	指定 Tunnel 的源地址或源接口
ipv6 enable	使能接口的 IPv6 功能
ipv6 address {ipv6-addressprefix-length | ipv6-address/prefix-length}	设置 Tunnel 接口的 IPv6 地址

2. ISATAP 隧道配置

站内自动隧道寻址协议(Intra-Site Automatic Tunnel Addressing Protocol，ISATAP)过渡技术采用了双栈和隧道技术实现从 IPv4 向 IPv6 的过渡。ISATAP 隧道是点到点的自动隧道技术，它将 IPv4 地址置入 IPv6 地址中，当两台 ISATAP 主机通信时，可自动抽取出 IPv4 地址建立 Tunnel 通信，并且不需要通过其他特殊网络设备，只要彼此间 IPv4 网络通畅即可。

当双栈主机使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的地址——ISATAP 地址。ISATAP 地址格式为 Prefix (64bit)：0:5EFE:IPv4ADDR，其中，0:5EFE 是 IANA 规定的格式，IPv4ADDR 是单播 IPv4 地址，它嵌入到 IPv6 地址的低 32 位。ISATAP 地址的前 64 位是通过向 ISATAP 路由器发送请求得到的，如果需要和其

他网络的 ISATAP 客户端或者 IPv6 网络通信，必须通过 ISATAP 路由器拿到全球单播地址前缀(2001：、002:、3ffe:开头)，通过路由器与其他 IPv6 主机和网络通信。

ISATAP 隧道可以用于 IPv4 网络中 IPv6 路由器与 IPv6 路由器、主机与路由器的连接。由于不要求隧道节点具有全球唯一的 IPv4 地址，可以用于内部私有网络中各双栈主机进行 IPv6 通信，所以 ISATAP 隧道适用于 IPv4 网络中 IPv6 主机之间的通信或 IPv4 网络中 IPv6 主机接入到 IPv6 网络的通信。ISATAP 隧道的相关配置命令及功能如表 10-8 所示。

表 10-8　ISATAP 隧道相关配置命令及功能

命　令	功　能
tunnel-protocol ipv6-ipv4 isatap	配置 Tunnel 接口的隧道协议为 ipv6-ipv4 并使用 isatap 隧道
ipv6 address 2001::/64 eui-64	配置接口的 EUI-64 格式的全球单播地址
source gigabitethemet 2/0/0	用来配置 Tunnel 源地址或源接口
Undo ipv6 ndra halt	用来使能系统发布 RA 报文功能
netsh interface ipv6 isatap set router	用来为用户端添加静态路由(Windows)
display ipv6 interface Tunnel 0/0/2	用来查看接口的 IPv6 信息

10.8　访问控制列表

10.8.1　考点辅导

10.8.1.1　ACL 的基本概念

IP 访问控制列表的过滤功能，提供了基于源地址、目的地址、各种协议和端口号的过滤准则。设定不同的过滤准则，不但能够实现拒绝接收或允许接收某些源 IP 地址的数据包进入路由器，也可以拒绝接收或允许接收到达某些目的 IP 地址的数据包通过路由器，还可以拒绝接收或允许接收某些协议的数据包通过路由器，拒绝接收或允许接收某些协议的某些端口号的数据包通过路由器。

IP 访问控制列表主要有两种类型：一类是标准访问控制列表(IP Standard Access Control List)；另一类是扩展访问控制列表(IP Extended Access Control List)。

(1) 标准访问控制列表只对数据包中的源地址进行检查，而不考虑目的地址及端口号等过滤选项，表号为 1～99。

(2) 扩展访问控制列表除了检查源地址和目的地址外，还可以检查指定的协议，根据数据包头中的协议类型进行过滤；可以检查端口号，根据端口号对数据包进行过滤。扩展访问控制列表的表号范围是 100～199，后来又进行了扩展，扩展的表号是 2000～2699。

10.8.1.2　ACL 配置命令

使用编号(2000～2999)创建一个数字型的基本 ACL，并进入基本 ACL 视图，操作命令如下：

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

或者使用名称创建一个命名型的基本 ACL，并进入基本 ACL 视图操作命令为：

```
acl name acl-name { basic| acl-number } [ match-order { auto | config } ]
```

如果创建 ACL 时未指定 match-order 参数，则该 ACL 默认的规则匹配顺序为 config；创建 ACL 后，ACL 的默认步长为 5。如果该值不能满足管理员部署 ACL 规则的需求，则可以对 ACL 步长值进行调整；(可选)执行命令 description text，配置 ACL 的描述信息。

配置基本 ACL 规则的操作命令如下：

```
rule [ rule-id ] { deny | permit } [ source { source-address source-wildcard
| any } |vpn-instance
vpn-instance-name | [ fragment | none-first-fragment ] | logging | time-range
time-name ]
```

以上步骤仅是一条 permit/deny 规则的配置步骤。实际配置 ACL 规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

1)　ACL 语句的删除

删除 ACL，系统视图下执行命令：

undo acl { [number] acl-number | all } 或 undo acl name acl-name

一般可以直接删除 ACL，不受引用 ACL 的业务模块影响(简化流策略中引用 ACL 指定 rule 的情况除外)，即无须先删除引用 ACL 的业务配置。

2)　调整 ACL 步长

在网络维护过程中，需要管理员为原 ACL 添加新的规则。由于 ACL 的默认步长是 5，在系统分配的相邻编号的规则之间，最多只能插入 4 条规则。调整步长，在 ACL 视图下执行 step　step，配置 ACL 步长。

3)　查看与清除 ACL 信息

确认设备 ACL 资源的分配情况，在任意视图下查看 ACL 资源信息的命令如下。

```
display acl resource [ slot slot-id ]
```

若显示信息中的计数非零，表示设备仍存在空余的 ACL 资源。

确认需要清除 ACL 的运行信息后，在用户视图下清除 ACL 统计信息的命令如下。

```
reset acl counter { name acl-name | acl-number | all }
```

4)　通配符掩码

ACL 规定使用通配符掩码来说明子网地址，通配符掩码就是子网掩码按位取反的结果。通配符掩码 0.0.0.0 表示 ACL 语句中的 32 位地址要求全部匹配，因而叫作主机掩码。例如：192.168.1.1　0.0.0.0 表示主机 192.168.1.1 的 IP 地址，实际上路由器把这个地址转换为 host 192.168.1.1，注意这里的关键字 host。

通配符掩码 255.255.255.255 表示任意地址都是匹配的，通常与地址 0.0.0.0 一起使用，例如：0.0.0.0 255.255.255.255，路由器将把这个地址转换为关键字 any。表 10-9 给出了几个使用通配符掩码的例子。

表 10-9　通配符掩码的例子

IP 地址	通配符掩码	匹　配
0.0.0.0	255.255.255.255	匹配任何地址(关键字 any)
172.16.1.1	0.0.0.0	匹配 host 172.16.1.1
172.16.1.0	0.0.0.255	匹配子网 172.16.1.0/24
172.16.2.0	0.0.1.255	匹配子网 172.16.2.0/23 (172.16.2.0-172.16.3.255)
172.16.0. 0	0.0.255.255	匹配子网 172.16.0.0/16 (172.16.0.0-172.16.255.255)

10.8.2　典型例题分析

例 10-23　利用扩展 ACL 禁止用户通过 telnet 访问子网 202.112.111.0/24 的命令是__(48)__。(2014 年下半年真题 48)

A. access-list 110 deny telnet any 202.112.111.0 0.0.0.255 eq 23

B. access-list 110 deny udp any 202.112.111.0 eq telnet

C. access-list 110 deny tcp any 202.112.111.0 0.0.0.255 eq 23

D. access-list 110 deny tcp any 202.112.111.0 255.255.255.0 eq 23

解析：扩展访问控制列表的表号范围是 100～199，扩展 ACL 的配置命令为:

```
Router(config)#ip access-list extended ACL_name
Router(config-std-acl)# permit/deny IP-protocol
source_address source_wildcard_mask [protocol_information]
destination_address destination_wildcard_mask [protocol_information] [log]
```

答案：C

例 10-24　每一个访问控制列表(ACL)最后都隐含着一条__(57)__语句。(2014 年下半年真题 57)

A. deny any　　B. deny all　　C. permit any　　D. permit all

解析：访问控制列表(ACL)是应用在路由器接口上的指令列表。这些指令列表用来告诉路由器哪些数据包可以接收，哪些数据包需要拒绝。至于数据包是被接收还是拒绝，可以由类似于源地址、目的地址、端口号等的特定指示条件来判断决定。

将数据包和访问控制列表进行比较时应遵循的重要规则如下。

(1)　数据包到来，则按顺序比较访问控制列表的每一行。

(2)　按顺序比较访问控制列表的各行，直到找到匹配的一行，一旦数据包和某行匹配，执行该行规则，不再进行后续比较。

(3)　最后一行隐含“deny”的意义。如果数据包与访问控制列表中的所有行都不匹配，将被丢弃。

(4)　IP 访问控制列表会发送一个 ICMP 主机不可达的消息到数据包的发送者，然后丢弃数据包。

(5)　如果某个访问控制列表挂接在实际接口上，删除列表后，默认的 deny any 规则会阻断那个接口的所有数据流量。

答案：A

例 10-25　以下关于访问控制列表的论述中，错误的是__(58)__。(2014 年下半年真题 58)

A. 访问控制列表要在路由器全局模式下配置

B. 具有严格限制条件的语句应放在访问控制列表的最后

C. 每一个有效的访问控制列表至少应包含一条允许语句

D. 访问控制列表不能过滤由路由器自己产生的数据

解析：设置访问控制列表的最关键的命令是 permit 和 deny。它们用来表示满足访问表项的报文是允许通过接口，还是要过滤掉。permit 表示允许报文通过接口，而 deny 表示匹配标准 IP 访问表源地址的报文要被丢弃。访问控制列表的条件语句是从第一句开始顺序执行的，只有与这个判断不相符合，才继续往下执行条件语句。

访问控制列表的配置工作的步骤主要包括：先定义一个标准、扩展或命名的访问控制列表；接着为该访问控制列表配置包过滤的准则；最后为这个访问控制列表配置应用接口。

答案：B

10.8.3　同步练习

1.　以下 ACL 语句中，含义为“允许 172.1610.0.0/24 网段所有 PC 访问 10.1.0.10 中的 FTP 服务”的是________。

A. access-list 101 deny tcp 172.1610.0.0 0.0.0.255 host 10.1.0.10 eq ftp

B. access-list 101 permit tcp 172.1610.0.0 0.0.0.255 host 10.1.0.10 eq ftp

C. access-list 101 deny tcp host 10.1.0.10 172.1610.0.0 0.0.0.255 eq ftp

D. access-list 101 permit tcp host 10.1.0.10 172.1610.0.0 0.0.0.255 eq ftp

2.　将 ACL 应用到路由器接口的命令是________。

A. Router(config-if)# ip access-group 10 out

B. Router(config-if)# apply access-list 10 out

C. Router(config-if)# fixup access-list 10 out

D. Router(config-if)# route access-group 10 out

3.　汇聚层交换机应该实现多种功能，下面的选项中，不属于汇聚层功能的是________。

A. VLAN 间的路由选择　　B. 用户访问控制

C. 分组过滤　　D. 组播管理

4.　访问控制列表(ACL)分为标准访问控制列表和扩展访问控制列表两种。下面关于 ACL 的描述中，错误的是________。

A. 标准 ACL 可以根据分组中的 IP 源地址进行过滤

B. 扩展 ACL 可以根据分组中的 IP 目标地址进行过滤

C. 标准 ACL 可以根据分组中的 IP 目标地址进行过滤

D. 扩展 ACL 可以根据不同的上层协议信息进行过滤

10.8.4 同步练习参考答案

1. B　　2. A　　3. B　　4. C

10.9 本 章 小 结

本章知识点在 2014 年的新大纲中改动不大，主要是知识点的明确化、具体化。

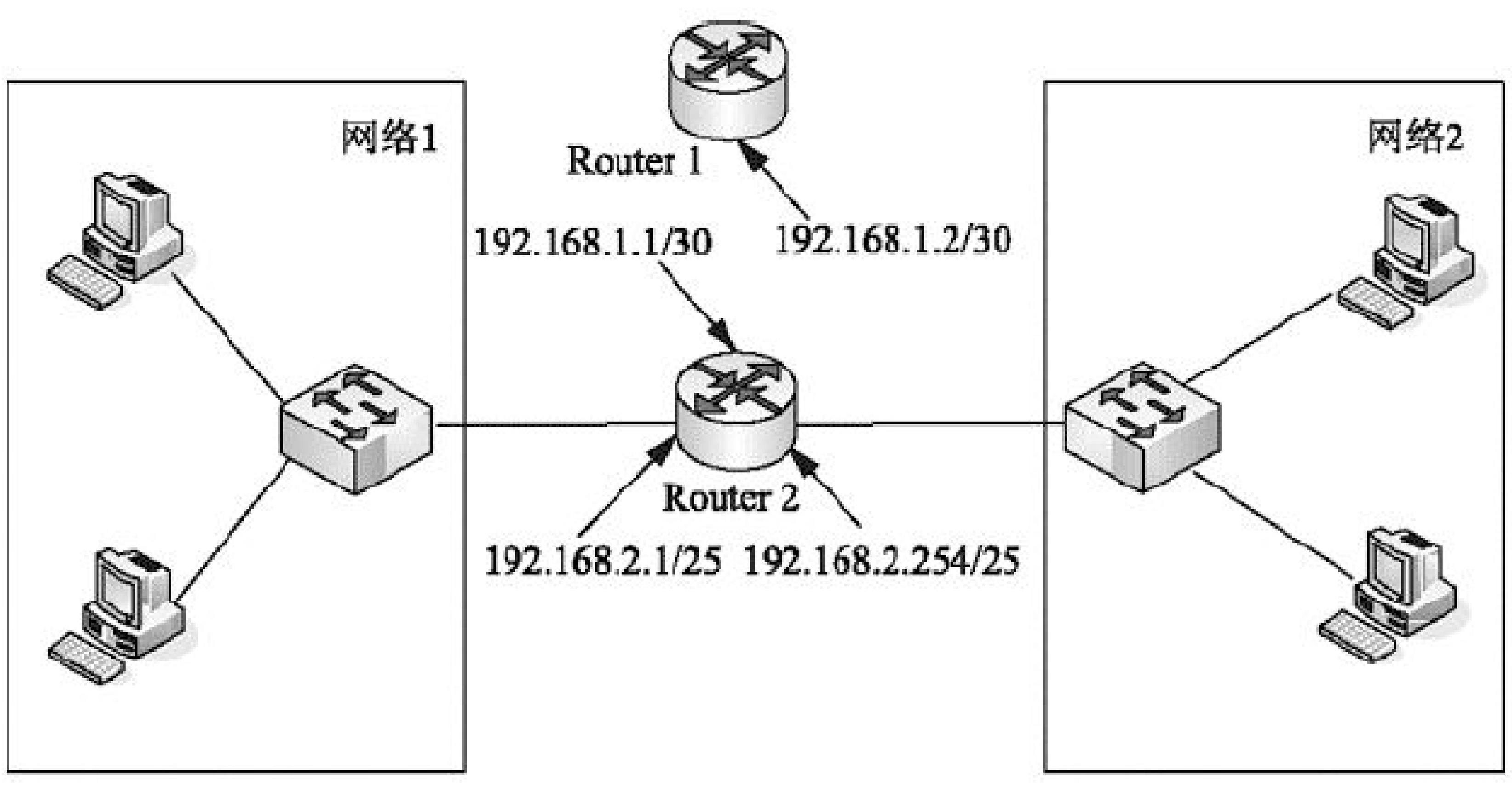
本章要求考生掌握组网技术的相关知识，包括交换机和路由器的配置、远程访问服务器、多层交换机功能和机制、IP 路由器功能和控制。

本章相关知识点在历次考试中分布相对集中，分值在 8 分左右，是考试的重点。根据往年的考题，本章每节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

10.10 达标训练题及参考答案

10.10.1 达标训练题

1. 在交换网络中，VTP 的作用是________。
   A. 选举根网桥　　B. 将 VLAN 信息传播到整个网络
   C. 建立端到端连接　　D. 选择最佳路由
2. 生成树协议(STP)使用参数________来选举根网桥。
   A. 网桥优先级和 IP 地址　　B. 链路速率和 IP 地址
   C. 链路速率和 MAC 地址　　D. 网桥优先级和 MAC 地址
3. 网络配置如下图所示，为路由器 Router 1 配置访问网络 1 和网络 2 的命令是__(1)__。路由配置完成后，在 Router 1 的__(2)__可以查看路由，查看路由采用的命令是__(3)__。



(1) A. ip route 192.1610.2.0 255.255.255.0 192.1610.1.1
    B. ip route 192.1610.2.0 255.255.255.128 192.1610.1.2

C. ip route 192.1610.1.0 255.255.255.0 192.1610.1.1

D. ip route 192.1610.2.128 255.255.255.128 192.1610.1.2

(2) A. 仅 Router1#模式下

B. Router1>或 Router1#模式下

C. Router1(config)#模式下

D. Router1(config-if)#模式下

(3) A. config/all　　B. route display　　C. show ip route　　D. show route

4. 配置路由器默认路由的命令是__________。

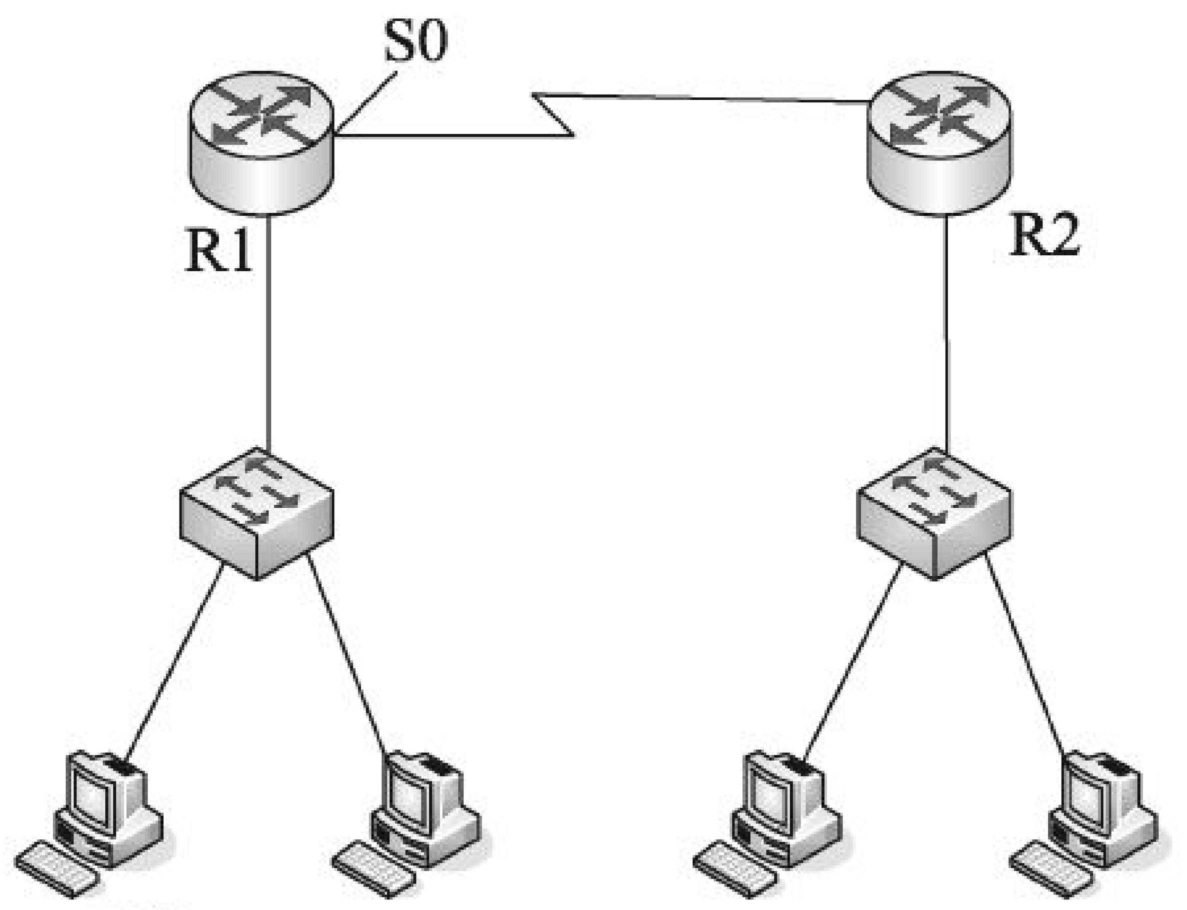
A. ip route 220.117.15.0 255.255.255.0 0.0.0.0

B. ip route 220.117.15.0 255.255.255.0 220.117.15.1

C. ip route 0.0.0.0 255.255.255.0 220.117.15.1

D. ip route 0.0.0.0 0.0.0.0 220.117.15.1

5. 某网络拓扑结构如下图所示。



在路由器 R2 上采用命令__(1)__得到如下所示结果。

```
R2>
…
R   192.1610.0.0/24[120/1] via 202.117.1121, 00:00:11, Serial2/0
C   192.1610.1.0/24 is directly connected, FastEthernet0/0
    202.117.112.0/30 is subnetted, 1 subnets
C   202.117.112.0 is directly connected, Serial2/0
R2>
```

则 PC1 可能的 IP 地址为__(2)__，路由器 R1 的 S0 接口的 IP 地址为__(3)__，路由器 R1 和 R2 之间采用的路由协议是__(4)__。

(1) A. netstat-r　　B.show ip route　　C. ip routing　　D. route print

(2)、(3) A. 192.1610.0.1　　B. 192.1610.1.1　　C. 202.117.112.1　　D. 202.117.112.2

(4) A. OSPF　　B. RIP　　C. BGP　　D. IGRP

6. 路由表如下所示，如果一个分组的目标地址是 220.117.5.65，则会被发送给________端口。

```
Network               Interface       next-hop
220.117.1.0/24        e0              directly connected
```

```
220.117.2.0/24        e0          directly connected
220.117.3.0/25        s0          directly connected
220.117.4.0/24        s1          directly connected
220.117.5.0/24        e0          220.117.1.2
220.117.5.64/28       e1          220.117.2.2
220.117.5.64/29       s0          220.117.3.3
220.117.5.64/27       s1          220.117.4.4
```

A. 220.117.1.2　　B. 220.117.2.2
C. 220.117.3.3　　D. 220.117.4.4

7. 以下关于两种路由协议的叙述中，错误的是______。
A. 链路状态协议在网络拓扑发生变化时发布路由信息
B. 距离矢量协议是周期性地发布路由信息
C. 链路状态协议的所有路由器都发布路由信息
D. 距离矢量协议是广播路由信息

8. RIP 是一种基于 (1) 算法的路由协议，一个通路上最大跳数是 (2) ，更新路由表的原则是到各个目标网络的 (3) 。
(1) A. 链路状态　B. 距离矢量　C. 固定路由　D. 集中式路由
(2) A. 7　B. 15　C. 31　D. 255
(3) A. 距离最短　B. 时延最小　C. 流量最小　D. 路径最空闲

9. OSPF 协议使用 (1) 报文来保持与其邻居的连接。下面关于 OSPF 拓扑数据库的描述中，正确的是 (2) 。
(1) A. Hello　B. Keepalive　C. SPF　D. LSU
(2) A. 每一个路由器都包含了拓扑数据库的所有选项
B. 在同一区域中的所有路由器包含同样的拓扑数据库
C. 使用 Dijkstra 算法来生成拓扑数据库
D. 使用 LSA 分组来更新和维护拓扑数据库

10. 路由器命令“Router(config)# access-list l deny 192.1610.1.1”的含义是______。
A. 不允许源地址为 192.1610.1.1 的分组通过
B. 允许源地址为 192.168.1.1 的分组通过
C. 不允许目标地址为 192.1610.1.1 的分组通过
D. 允许目标地址为 192.1610.1.1 的分组通过

10.10.2 参考答案

1. B　2. D　3. (1) A　(2) B　(3) C　4. D
5. (1) B　(2) A　(3) D (4) B　6. C　7. C
8. (1) B　(2) B　(3) A　9. (1) A　(2) D　10. A

第 11 章　网 络 管 理

大纲要求：

- 网络管理的功能域。
- 网络管理协议。
- 网络管理命令。
- 网络管理工具。
- 网络管理平台。
- 分布式网络管理。

11.1　网络管理系统体系结构

11.1.1　考点辅导

1. 网络管理系统的层次结构

网络管理系统组织成图 11-1 所示的层次结构。在网络管理站中最下层是操作系统和硬件。操作系统之上是支持网络管理的协议簇，如 OSI、TCP/IP 等通信协议以及专用于网络管理的 SNMP、CMIP 协议等。

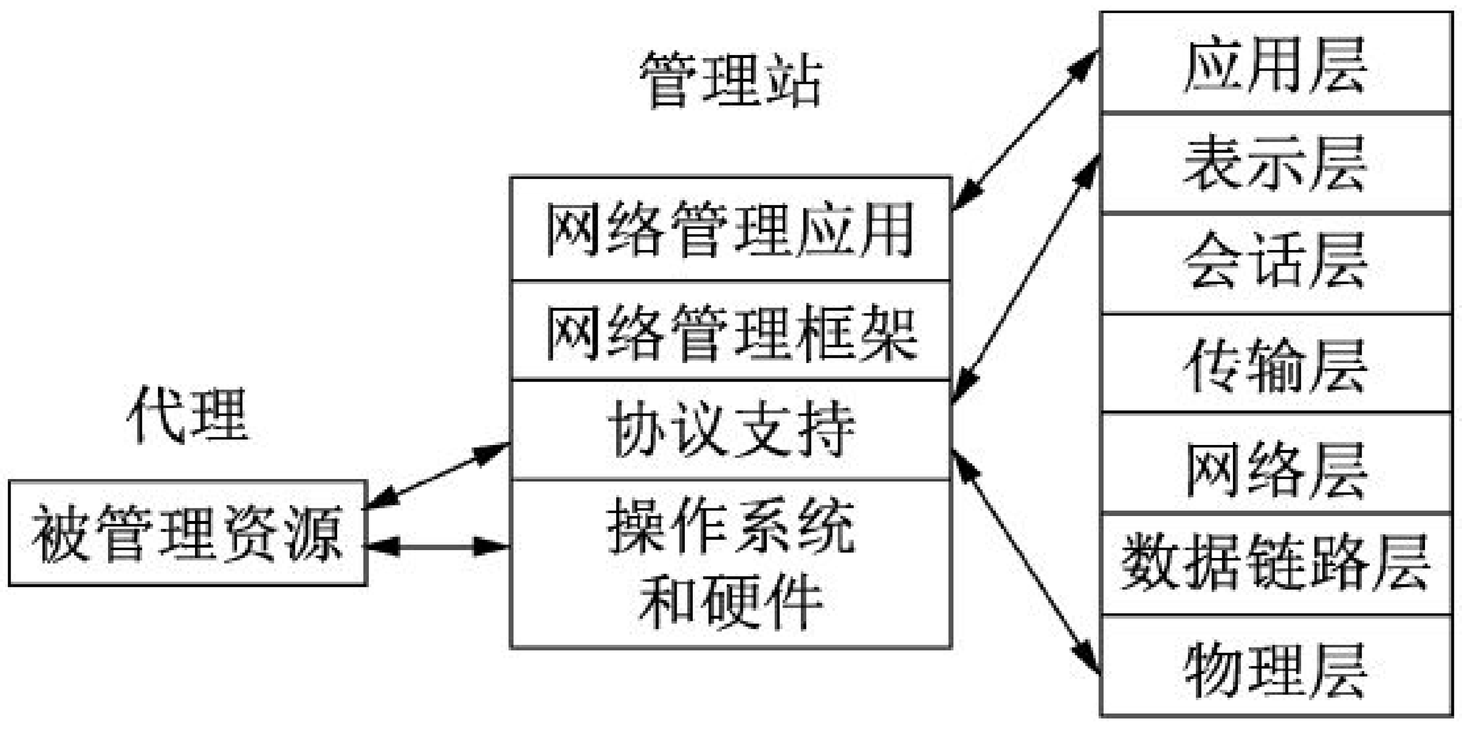


图 11-1　网络管理系统的层次结构

网络管理框架(Network Management Framework)是各种网络管理应用工作的基础结构。网络管理框架具有以下特点。

- 管理功能分为管理站(Manager)和代理(Agent)。
- 为存储管理信息提供数据库。
- 提供用户接口和用户视图功能。
- 提供基本的管理操作。

网络管理应用实现特定的管理目标，包括性能监测、故障诊断、业务管理和安全控制。

2. 网络管理系统的配置

一个完整的网络管理系统由多个部件组成，主要包括网络管理协议、网络管理工作站、被管网络部件、管理信息库(MIB)。

作为管理者(Manager)，一个网络系统中可以有一个(或者几个)网络管理工作站；被管理者称为代理(Agent)，网上具有多个被管网络部件；网络管理协议是管理者和被管理者之间的操作规范，具体的操作对象则是管理信息的集合——管理信息库(Management Information Base，MIB)。

网络管理系统的基本工作流程如下。

(1) 在被管理部件上预置代理。

(2) 网络管理者使用网络管理协议从代理的 MIB 中取得被管网络部件的管理信息，并存入自己的 MIB。

(3) 管理软件通过对 MIB 的分析处理，达到网络监控的管理目的。

3. 网络管理软件的结构

这里所说的网络管理软件包括用户接口软件、管理专用软件和管理支持软件，如图 11-2 所示。

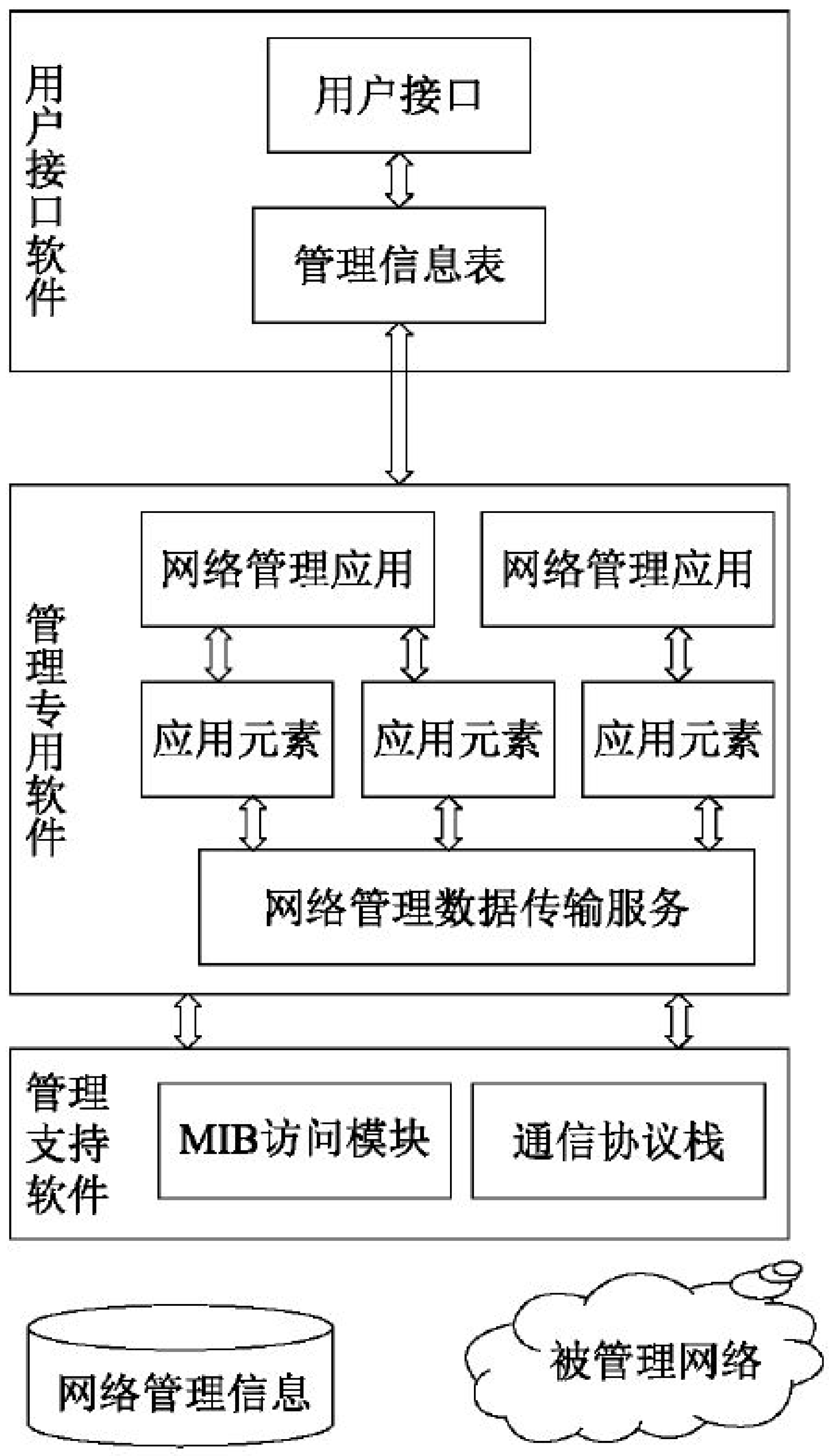


图 11-2 网络软件结构

用户通过网络管理接口与管理专用软件交互作用，监视和控制网络资源。用户接口软件不但存在于管理主机上，而且也可能出现在网管代理系统中，以便对网络资源实施本地配置、测试和排错。

用户接口软件应具备下列特点。

(1) 统一的用户接口。不论主机和设备出自何方厂家，运行什么操作系统，都需要统一的用户接口，这样才可以方便地对异构型网络进行监控。

(2) 具备一定的信息处理能力。对大量的管理信息要进行过滤、统计、求和，甚至进行简化，以免传递的信息量太大而阻塞网络通道。

(3) 图形用户接口。具有非命令行或表格形式的用户操作维护界面。

复杂的网络管理软件可以支持多种网络管理应用，如配置管理、性能管理和故障管理等。这些应用适用于各种网络设备和网络配置，虽然在实现细节上可能有所不同。

管理支持软件包括 MIB 访问模块和通信协议栈。网管代理中的 MIB 包含反映设备配置和设备行为的信息以及控制设备操作的参数。管理站的 MIB 中除保存本地节点专用的管理信息外，还保存着管理站控制的所有网管代理的有关信息。MIB 访问模块具有基本的文件管理功能，使得管理站或网管代理可以访问 MIB，同时该模块还能把本地的 MIB 数据转换成适用于网络管理系统传送的标准格式。通信协议栈支持节点之间的通信。由于网络管理协议位于应用层，原则上任何通信体系结构都能胜任，虽然具体的实现可能有特殊的通信需求。

11.1.2　典型例题分析

例 11-1　下列不属于用户接口软件的特点的是________。

A. 统一的用户接口　　　　　　B. 具备一定的信息处理能力

C. 图形用户接口　　　　　　　D. 独特的用户接口

解析：用户接口软件应具备下列特点：统一的用户接口，具备一定的信息处理能力，图形用户接口。

答案：D

11.1.3　同步练习

一个完整的网络管理系统由多个部件组成，下列不属于网络管理系统部件的是________。

A. 网络管理协议　　　　　　　B. 用户接口

C. 被管网络部件　　　　　　　D. 管理信息库(MIB)

11.1.4　同步练习参考答案

B

11.2　网络监控系统的组成

11.2.1　考点辅导

11.2.1.1　管理信息的组成

对网络监控有用的管理信息可以分为以下 3 类。

(1) 静态信息：系统和网络的配置信息，如路由器的端口数和编号、CPU 的类型。

(2) 动态信息：网络和设备运行和工作的状态，如网络中传送的分组数、网络连接的状态。

(3) 统计信息：从动态信息统计出来的信息，如每分钟发送的分组数、传输失败的概率。

这些信息组成的管理信息库如图 11-3 所示。

配置数据库存储着设备和网络的基本配置信息，传感器数据库存储着传感器的设置信息。

传感器是一组软件，用于实时地读取被管设备的参数。

动态数据库存储着由传感器收集的各种网络元素和网络事件的实时数据。

统计数据库中的管理信息是由动态数据库的信息计算出来的。

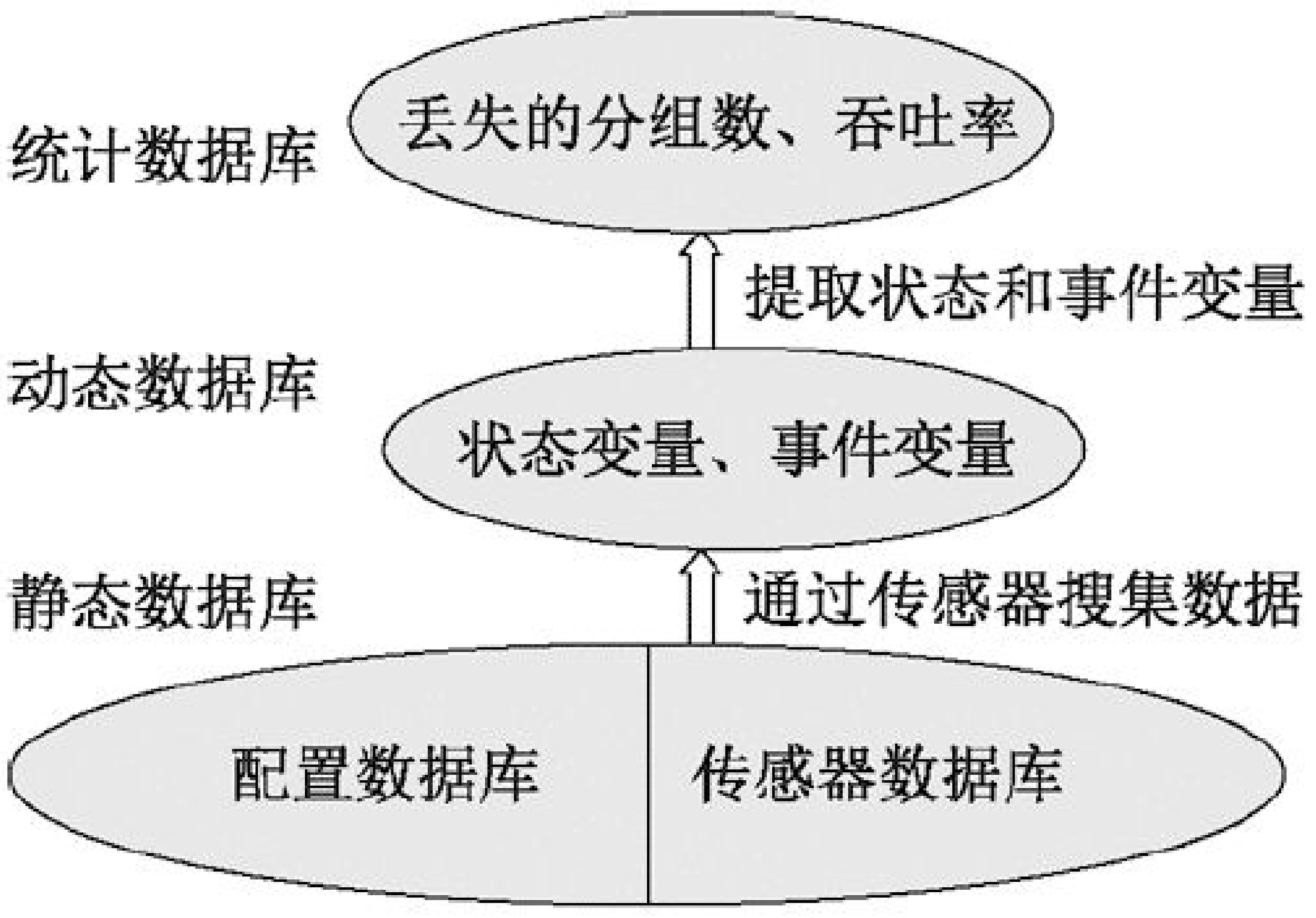


图 11-3　管理信息库的组成

11.2.1.2　网络监控系统的配置

网络监控系统的配置如下。

(1) 静态信息由网络元素直接产生，由驻留在网络元素中的代理(委托代理)进程收集存储。

(2) 动态信息由产生相关事件的网络元素收集和存储，也可以由管理站收集和存储。

(3) 统计信息一般由网络的管理站产生和存储。

11.2.1.3　网络监控系统的通信机制

1. 轮询

轮询是一种请求—响应式的交互方式。管理站向代理发出请求，询问(管理站)所需要的信息值，代理响应管理站，从管理信息库中取得相应的信息，返回给管理站。

2. 事件报告

代理根据管理站的要求，向管理站主动发送状态报告。当代理检测到某些报告时，则向管理站发送。

11.2.2　典型例题分析

例 11-2　某局域网采用 SNMP 进行网络管理，所有被管设备在 15min 内轮询一次，网络没有明显拥塞，单个轮询时间为 0.4s，则该管理站最多可支持_______个设备。

A. 18 000　　B. 3600　　C. 2250　　D. 90 000

解析：管理站支持的设备数 N 与轮询间隔 T、单个轮询需要的时间Δ之间的关系为 $N \leqslant T/\Delta$。

本题中，T=15×60，Δ=0.4，可得 $N \leqslant 2250$，因此管理站最多可支持的设备个数为 2250。

答案：C

11.2.3　同步练习

对网络监控有用的管理信息可以分为以下 3 类，下列不符合的是________。

A. 静态信息　　B. 动态信息　　C. 统计信息　　D. 存储信息

11.2.4　同步练习参考答案

D

11.3　网络管理功能域

11.3.1　考点辅导

1. 性能管理

性能管理用来保证有效地运营网络并提供约定的服务质量。在保证各种业务的服务质量(QoS)的同时，尽量提高网络资源的利用率。性能管理包括性能监测功能、性能分析功能和性能管理控制功能。

2. 故障管理

故障管理的作用是迅速发现和纠正网络故障，动态维护网络的有效性。故障管理的主要功能有报警监测、故障定位、测试、业务恢复及修复等，同时还有维护故障日志的功能。

3. 计费管理

计费管理的作用是正确地计算和收取用户使用网络服务的费用，进行网络资源利用率的统计和网络的成本效益核算。计费管理主要提供费率管理功能和账单管理功能。

4. 配置管理

配置管理是最基本的网络管理功能，负责监测和控制网络的配置状态。具体地讲，就是在网络建立、扩充、改造及业务的开展过程中，对网络的拓扑结构、资源配备、使用状态等配置信息进行定义、监测和修改。

5. 安全管理

安全管理的作用是提供信息的保密、认证和完整性保护机制，使网络中的服务、数据和系统免受侵扰和破坏。安全管理主要包含风险分析功能，安全服务功能，告警、日志和报告功能以及网络管理系统保护功能。

11.3.2 典型例题分析

例 11-3 网络管理系统中故障管理的目标是 (46) 。(2015 年上半年真题 46)

A. 自动排除故障　　B. 优化网络性能

C. 提升网络安全　　D. 自动监测故障

解析：故障管理是网络管理中最基本的内容之一。故障管理的目的在于确保网络系统的高稳定性。在网络出现故障时，故障管理系统必须及时发现故障部位。故障管理的日常工作包含对所有节点动作状态的监控、故障记录的追踪与检查，以及平常对网络系统的测试。

答案：D

11.3.3 同步练习

1. 下列说法错误的是________。

A. 性能管理用来保证有效地运营网络并提供约定的服务质量

B. 故障管理的作用是迅速发现和纠正网络故障，动态维护网络的有效性

C. 计费管理的作用是正确地计算和收取用户使用网络服务的费用

D. 安全管理是最基本的网络管理功能，负责监测和控制网络的配置状态

2. OSI 定义的网络管理包括配置管理、故障管理、性能管理、计费管理和安全管理五大功能，下列操作中属于配置管理的是______。

A. 网络管理者通过 GetRequest 获得当前处理的消息数据

B. 网络管理者通过 GetRequest 获得计费参数

C. 网络管理者通过 SetRequest 更改系统的 LOG 级别

D. 网管代理通过 Trapani 发送故障消息

11.3.4 同步练习参考答案

1. D　2. C

11.4 简单网络管理协议

11.4.1 考点辅导

11.4.1.1 SNMPv1

Internet 最初的网络管理框架由 4 个文件定义，如图 11-4 所示，这就是 SNMP 第 1 版。RFC1155 定义了管理信息结构(SMI)，即规定了管理对象的语法和语义。SMI 主要说

明了怎样定义管理对象和怎样访问管理对象。RFC1212 说明了定义 MIB 模块的方法，而 RFC1213 则定义了 MIB-Ⅱ管理对象的核心集合，这些管理对象是任何 SNMP 系统必须实现的。RFC1157 是 SNMPv1 的规范文件。

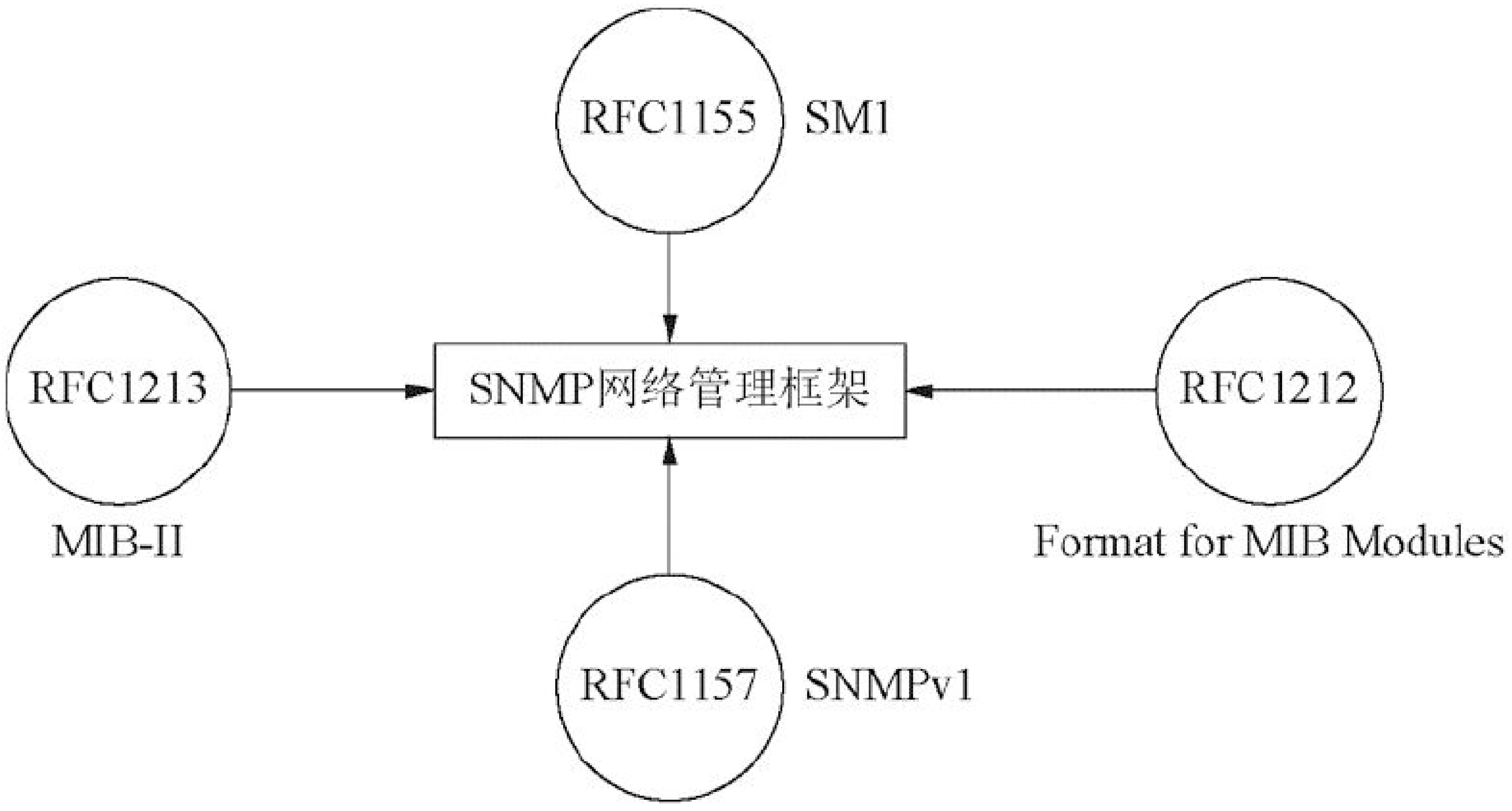


图 11-4　SNMP 网络管理框架的定义

SNMP 的通信基础是 TCP/IP，它利用了传输层上的用户数据报协议(UDP)。SNMP 的协议体系结构如图 11-5 所示。

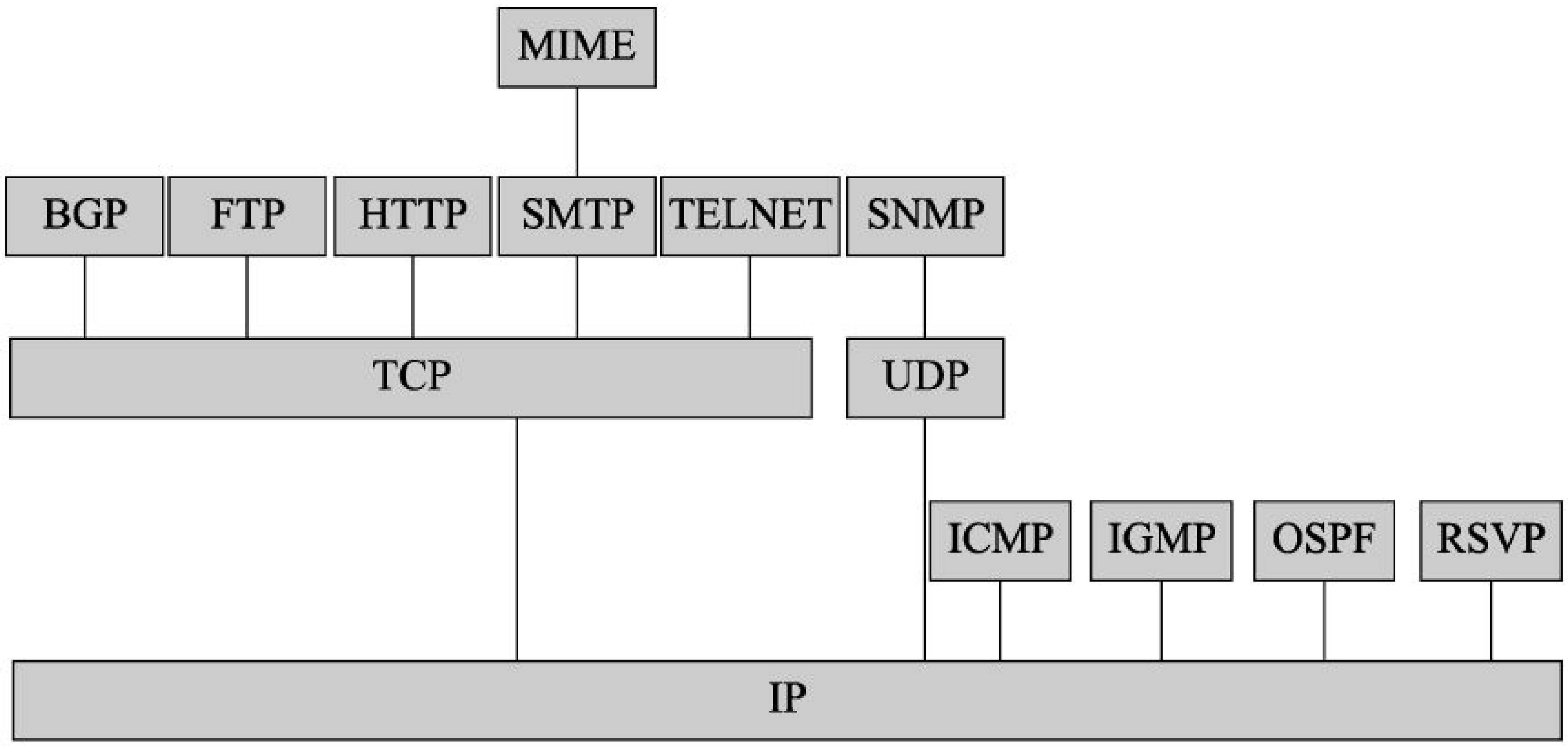


图 11-5　SNMP 的通信基础

其中的一些协议解释如下。

- BGP(Border Gateway Protocol)：边界网关协议。
- FTP(File Transfer Protocol)：文件传输协议。
- HTTP(HyperText Transfer Protocol)：超文本传输协议。
- SMTP(Simple Mail Transfer Protocol)：简单邮件传输协议。
- MIME(Multi-Purpose Internet Mail Extension)：多用途的网际邮件扩展。
- ICMP(Internet Control Message Protocol)：因特网控制报文协议。

11.4.1.2　SNMPv2

SNMPv2 的管理信息结构是在总结 SNMP 应用经验的基础上对 SNMPv1 SMI 进行了

扩充，提供了更精致、更严格的规范，规定了新的管理对象和MIB 的文档，可以说是 SNMPv1 SMI 的超集。SNMPv2 SMI 引入了 4 个关键的概念。

- 对象的定义。
- 表的定义。
- 通知的定义。
- 信息模块。

1. 对象的定义

对象的定义是使用对象语法来描述的。在每一个 MIB 内部的对象都有一个正式的定义，它规定了对象的数据类型、允许的形式、取值范围以及与其他 MIB 内部对象之间的关系。使用 ASN.1 符号定义了每一个对象，而且也定义了整个 MIB 的结构。为了保持对象的简单性，只是使用了 ASN.1 元素和特性的一个有限子集。其中对象的数据类型通常是 UNIVERSAL，但是在 MIB-Ⅱ中只有下列数据类型可用于 MIB 对象的定义。

- integer(UNIVERSAL 2)。
- octetstring(UNIVERSAL 4)。
- null(UNIVERSAL 5)。
- object identifier(UNIVERSAL 6)。
- sequence、sequence-of(UNIVERSAL 16)。

其中，前面 4 种是基本类型，是组成其他对象类型的基本块。sequence 和 sequence-of 用来构建表。

在 MIB-2 中，每个应用程序都定义了自己的 APPLICATION 数据类型。这里 APPLICATION 类型是 ASN.1 的 APPLICATION 类，它由与特定应用程序相关的数据类型组成。RFC1155 中定义的一些应用程序范围类型如下。

- networkaddress：使用 CHOICE 结构来定义，允许从许多协议组中选择一种地址格式。
- ipaddress：由 IP 定义的 32 位地址。
- counter：只能增加不能减少的非负整数。
- gauge：可增可减的非负整数。
- timeticks：计算从某一个时刻开始时间的非负整数，以 0.01s 为单位进行计算。
- opaque：该类型能够产生任意类型数据。

与 SNMPv1 一样，SNMPv2 也是用 ASN.1 宏定义 OBJECT-TYPE 表示管理对象的语法和语义，但是 SNMPv2 的 OBJECT-TYPE 增加了新的内容，如图 11-6 所示。

```
OBJECT-TYPEMACRO::=BEGIN
  TYPE NOTATION::="SYNTAX"Syntax
    UnitsPart
    "MAX-ACCESS"Access
    "STATUS"Status
    "DESCRIPTION"Text
    ReferPart
    IndexPart
    DefValPart
  VALUE NOTATION::=value (VALUE ObjectName)
END
```

图 11-6 SNMPv2 新添内容

对象宏定义说明如下。

- UnitsPart：在 SNMPv2 的 OBJECT-TYPE 宏定义中增加了 UNITS 子句。这个子句用文字说明与对象有关的度量单位。当管理对象表示一种度量手段(如时间)时，这个子句是有用的。
- MAX-ACCESS 子句：类似于 SNMPv1 的 ACCESS 子句，说明最大的访问级别，与授权策略无关。SNMPv2 定义的访问类型中去掉了 write-only 类，增加了一个与概念行有关的访问类型 read-create，表示可读、可写、可生成。还增加了 accessible-for-notify 访问类，这种访问方式与陷入有关。
- STATUS 子句：这个子句是必要的，也就是说必须指明对象的状态。新标准去掉了 SNMPv1 中的 optional 和 mandatory，只有 3 个可选的状态。如果说明管理对象的状态是 current，则表示在当前的标准中是有效的。如果管理对象的状态是 obsolete，表示不必实现这种对象。状态 deprecated 表示对象已经过时了，但是为了与旧的实现互操作，实现时还要支持这种对象。

其他子句的意义和 SNMPv1 相同。

2. 表的定义

由于 SMI 只支持简单的二维标量表这一种数据结构，因此，与 SNMPv1 一样，SNMPv2 的管理操作只能作用于标量对象，复杂的信息要用表来表示。按照 SNMPv2 规范，表是行的序列，而行是列对象的序列。SNMPv2 把表分为两类。

(1) 禁止删除和生成行的表。这种表的最高访问级别是 read-write。在很多情况下这种表由代理控制，表中只包含 read-only 型的对象。

(2) 允许删除和生成行的表。这种表开始时可能没有行，由管理站生成和删除行。行数可由管理站或代理改变。

在 SNMPv2 表的定义中必须含有 INDEX 或 AUGUMENTS 子句，但是只能有一个。INDEX 子句定义了一个基本概念行，而 INDEX 子句中的索引对象确定了一个概念行实例。与 SNMPv1 不同，SNMPv2 的 INDEX 子句中增加了任选的 IMPLIED 修饰符。假定一个对象的标识符为 y，索引对象为 i_1，i_2，…，i_N，则对象 y 的一个实例标识符为 $y.(i_1).(i_2).\cdots.(i_N)$。

SMI 中表的定义不允许嵌套，也就是说，不允许表中的元素又是另外一个表，这限制了 SMI 的性能和灵活性。

3. 表的操作

SNMPv2 允许生成和删除行的表必须有一个列对象，其 SYNTAX 子句的值为 RowStatus，MAX-ACCESS 子句的值为 read-write，这种列称为概念行的状态列。状态列可取 6 种值。

- active(可读写)：被管理设备可以使用概念行。
- notInService(可读写)：概念行存在，但由于其他原因(下面解释)而不能使用。
- notReady(只读)：概念行存在，但因没有信息而不能使用。
- createAndGo(只写不读)：管理站生成一个概念行实例时先设置成这种状态，生成过程结束时自动变为 active，被管理设备就可以使用了。
- createAndWait(只写不读)：管理站生成一个概念行实例时先设置成这种状态，但不

会自动变成 active。

- destroy(只写不读)：管理站需删除所有的概念行实例时设置成这种状态。

这 6 种状态中除 notReady 外的 5 种状态是管理站可以用 set 操作设置的状态，前 3 种可以是响应管理站的查询而返回的状态。

表中概念行的生成可以使用两种不同的方法，分成 4 个步骤。

(1) 选择实例标识符。针对不同的索引对象可考虑用不同的方法选择实例标识符。

(2) a 管理站通过事务处理产生和激活概念行。b 管理站与代理协商生成概念行。

(3) 初始化非默认值对象。管理站用 get 命令查询所有列，以确定是否能够或需要设置列对象的值。

(4) 激活概念行。

概念行的挂起：当概念行处于 active 状态时，如果管理站希望概念行脱离服务，以便进行修改，则可以发出 set 命令，把状态列由 active 置为 notInService。

概念行的删除：管理站发出 set 命令，把状态列置为 destroy，如果这个操作成功，概念行立即被删除。

4. 通知和信息模块

SNMPv2 提供了通知类型的宏定义 NOTIFICATION-TYPE，用于定义异常条件出现时 SNMPv2 实体发送的信息。

SNMPv2 还引入了信息模块的概念，用于说明一组有关的定义。共有以下 3 种信息模块。

- MIB 模块：包含一组有关的管理对象的定义。
- MIB 的依从性声明模块：使用 MODULE-COMPLIANCE 和 OBJECT-GROUP 宏说明有关管理对象实现方面的最小要求。
- 代理能力说明模块：用 AGENT-CAPABILITIES 宏说明代理实体应该实现的能力。

11.4.1.3 SNMPv3

在 SNMPv3 中，以前叫作管理站和代理的东西现在统一称为 SNMP 实体(SNMP Entity)。

实体是体系结构的一种实现，由一个或多个有关的 SNMP 引擎(SNMP Engine)和一个或者多个有关的 SNMP 应用(SNMP Application)组成。图 11-7 显示了 SNMP 实体的组成元素。

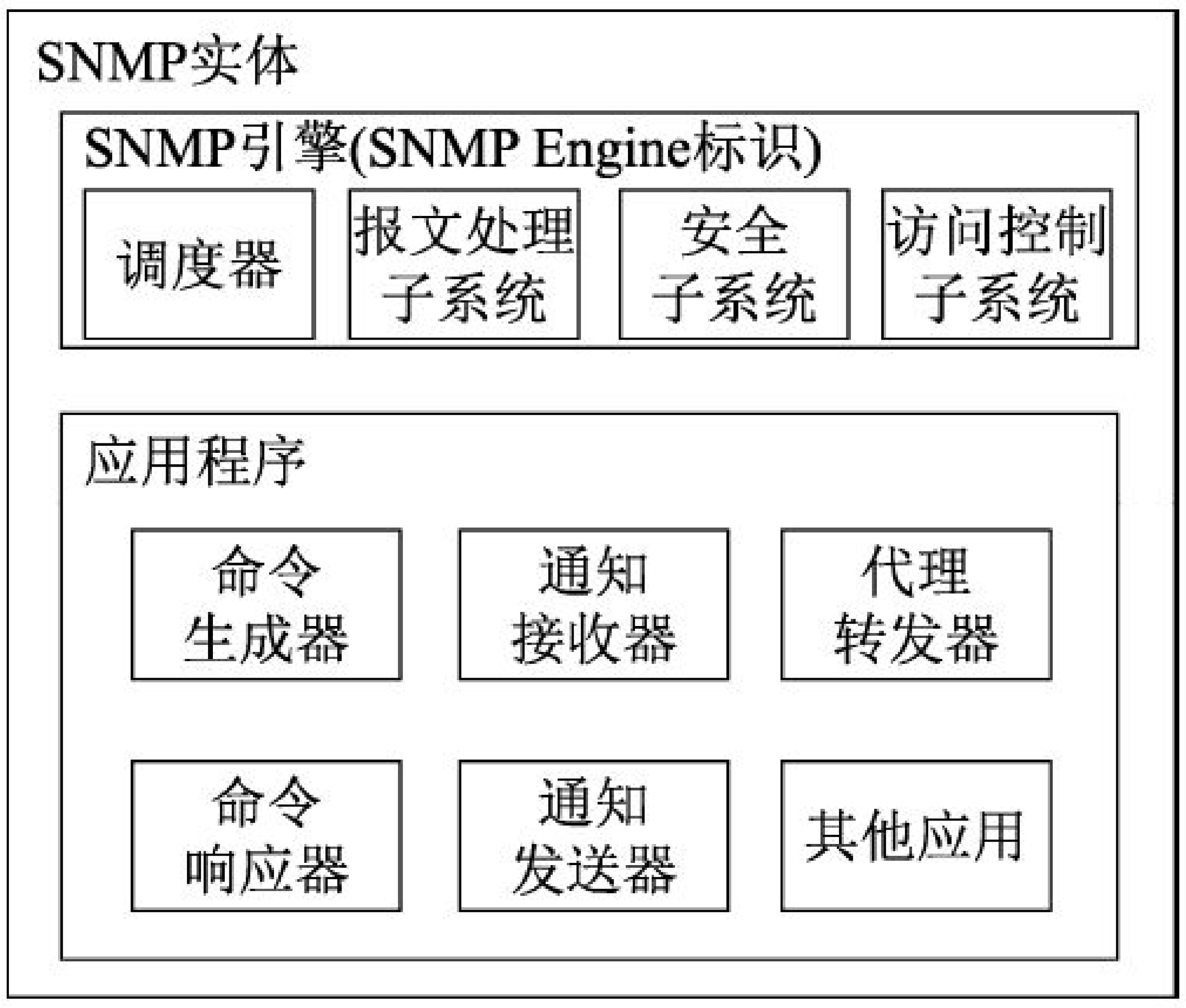


图 11-7 SNMP 实体组成元素

1. SNMP 引擎

SNMP 引擎提供下列服务。

- 发送和接收报文。
- 认证和加密报文。
- 控制对管理对象的访问。

SNMP 引擎有唯一的标识 snmpEngindID，这个标识在一个上层管理域中是无二义性的。

2. 应用程序

SNMPv3 的应用程序分为 5 种。

(1) 命令生成器(Command Generators)：建立 SNMP Read/Write 请求，并且处理对这些请求的响应。

(2) 命令响应器(Command Responders)：接收 SNMP Read/Write 请求，对管理数据进行访问，并按照协议规定的操作产生响应报文，返回读/写命令的发送者。

(3) 通知发送器(Notification Originators)：监控系统中出现的特殊事件，产生通知类报文，并且要有一种机制，以决定向何处发送报文，使用何种 SNMP 版本和安全参数等。

(4) 通知接收器(Notification Receivers)：监听通知报文，并产生响应。

(5) 代理转发器(Proxy Repeaters)：在 SNMP 实体之间转发报文。

11.4.2　典型例题分析

例 11-4　在 SNMP 协议中，代理收到管理站的一个 GET 请求后，若不能提供该实例的值，则__(46)__。(2017 年下半年真题 46)

A. 返回下个实例的值　　B. 返回空值　　C. 不予响应　　D. 显示错误

解析：正常情况下，返回管理站请求的每个值，如果不能够提供，没有相关值的时候，则返回下一个值。

答案：A

例 11-5　SNMP 是一种异步请求/响应协议，采用__(47)__协议进行封装。(2017 年下半年真题 47)

A. IP　　B. ICMP　　C. TCP　　D. UDP

解析：SNMP 在传输层使用的是 UDP 协议。

答案：D

例 11-6　SNMP 协议中网管代理使用__(47)__操作向管理站异步事件报告。(2016 年下半年真题 47)

A. trap　　B.set　　C. get　　D. get-next

解析：SNMP 使用的是无连接的 UDP，在运行代理程序的服务器端用 161 端口来接收 Get 或 Set 报文和发送响应报文(客户端使用临时端口)，但运行管理程序的客户端则使用熟悉的端口 162 来接收来自各代理的 Trap 报文。

答案：A

例 11-7　下列网络管理软件中不需要 SNMP 支持的是__(49)__。(2015 年下半年真题 49)

A. CiscoWorks　　B. Netview　　C. Solarwinds　　D. Wireshark

解析：本题考查网管命令网络管理软件的使用常识。

在这 4 个软件中，CiscoWorks、Netview 以及 Solarwinds 都是网络管理软件，都需得到 SNMP 的支持，而 Wireshark (前称 Ethereal)是一个网络封包分析软件。网络封包分析软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料，并不要求 SNMP 的支持。

答案：D

例 11-8　在 SNMPv2 错误类型中，表示管理对象不可访问的是__(50)__。(2015 年下半年真题 50)

A. noAccess　　B. genErr　　C. wrongValue　　D. noCreation

解析：本题考查 SNMPv2 的错误类型。

在 SNMPv2 错误类型中，表示管理对象不可访问的是 noAccess。而 genErr 表示某些其他的差错。若代理不执行该操作，则返回 wrongValue。noCreation 则表示对象不存在且无法建立。

答案：A

例 11-9　SNMP 属于__(44)__层协议。(2015 年上半年真题 44)

A. 物理　　B. 网络　　C. 传输　　D. 应用

解析：SNMP 定义在 OSI 模型的应用层，依赖于 UDP 数据报服务。SNMP 能够使网络管理员提高网络管理效能，及时发现并解决网络问题以及规划网络的增长。网络管理员还可以通过 SNMP 接收网络节点的通知消息以及告警事件报告等来获知网络出现的问题。

答案：D

例 11-10　SNMPv3 新增了__(45)__功能。(2015 年上半年真题 45)

A. 管理站之间通信　　B. 代理

C. 认证和加密　　D. 数据块检索

解析：SNMPv3 主要增加了 SNMP 在安全性和远端配置方面的功能。SNMPv3 提供重要的安全性功能如下。

信息完整性：保证封包在传送中没有被篡改。

认证：检验信息来自正确的来源。

封包加密：避免被未授权的来源窥探。

答案：C

11.4.3　同步练习

1. SNMPv2 的________操作为管理员提供了从被管设备中一次取回一大批数据的能力。

A. GetNextRequest　　B. InformRequest

C. SetRequest　　D. GetBulkRequest

2. SNMPc 支持各种设备访问方式，在 SNMPc 支持的设备访问方式中，只是用于对 TCP 服务轮询的方式是________。

A. 无访问模式　　B. ICMP(Ping)

C. SNMPv1 和 v2C　　　　D. SNMPv3

3. 下列数据类型中，SNMPv2 支持而 SNMPv1 不支持的是______。

A. OCTET STRING　　　　B. OBJECT descriptor

C. Unsigned32　　　　D. Gauge32

11.4.4 同步练习参考答案

1. D　　2. A　　3.C

11.5 管理数据库 MIB-Ⅱ

11.5.1 考点辅导

1. 被管理对象的定义

MIB 是网络管理系统中的重要构件，它由系统内许多被管理对象及其属性组成。被管理对象是指可使用管理协议进行管理和控制的网络资源的抽象表示。MIB 从概念上看实际上就是一个虚拟数据库，它提供有关被管理对象的信息，这些信息由管理进程和各个代理进程共享。

SNMP 中把所有管理对象组织成分层的树形结构，MIB 由一系列对象组成。这里对象是指通信和信息处理范畴中可标识的一切拥有一定信息特性的资源，它与面向对象系统中所定义的对象并不完全相同。每个对象属于一定的对象类型，并且有一个具体的值。对象类型的定义是一种语法描述，对象实例是对象类型的具体实现，只有实例才可以绑定到特定的值。

SNMP MIB 的宏定义最初在 RFC1155 中说明，称为 MIB-Ⅰ。后来对 RFC1212 进行了扩充，称为 MIB-Ⅱ。图 11-8 是 RFC1212 中对象类型的定义，对其中关键的子句解释如下。

- SYNTAX：表示对象类型的抽象语法。
- ACCESS：定义通过 SNMP 或者其他协议访问对象实例的方法。访问子句规定该对象类型所需要的最低级别的支持，在具体实现中可以增加或者限制访问，可选择的访问方式有只读(read-only)、读写(read-write)、只写(write-only)和不可访问(not-accessible)4 种。
- STATUS：指明了对象所需要的实现支持。状态子句中定义了必要的(Mandatory)和任选的(Optional)两种支持程度。过时的(Obsolete)是指旧标准支持而新标准不支持的类型。如果一个对象被说明为可取消的(Deprecated)，则表示当前必须支持这种对象，但在将来的标准中可能被取消。
- DescrPart：这个子句是任选的，用文字说明对象类型的含义。
- ReferPart：在其他 MIB 模块中定义的文本交叉索引。该子句是可选的。
- IndexPart：用于定义表对象的索引项，该子句只在对象类型符合概念行时出现。

- Def ValPart：定义可以接受的默认值，代理在创建实例时使用。该子句是可选的。
- VALUE NOTATION：规定用于通过 SNMP 访问该对象时使用的名称。

```
OBJECT-TYPE MACRO ::=
BEGIN
    TYPE NOTATION :: ="SYNTAX"type(TYPE ObjectSyntax)
     "ACCESS"Access
     "STATUS"Status
    DescrPart
    ReferPart
    IndexPart
    DefValPart
  VALUE NOTATION :: =value(VALUE ObjectName)
  Access :: ="read-only" |"read-write"|"write-only "|"not-accessible"
  Status :: ="mandatory" |"optional"|"obsolete "|"deprecated"
  DescrPart :: ="DESCRIPTION"value(description DisplayString)|empty
  ReferPart :: ="REFERENCE"value(reference DisplayString)|empty
  IndexPart:: ="INDEX""{"IndexTypes"}"
  IndexTypes :: =IndexType|IndexTypes","IndexType
  IndexType :: =value(indexobject ObjectName)|type(indextype)
  DefValPart :: ="DEFVAL""{"value(defvalue ObjectSyntax)"}"|empty
  DisplayString :: =OCTET STRING SIZE(0..255)
END
```

图 11-8　管理对象的宏定义(RFC1212)

2. MIB-Ⅱ的功能组

在 TCP/IP 网络管理的建议标准中，提出了多个相互独立的 MIB，其中包含为 Internet 的网络管理而开发的 MIB-Ⅱ。鉴于它在说明标准 MIB 的结构、作用和定义方法等方面的重要性和代表性，有必要对其进行比较深入的讨论。

MIB-Ⅱ是在 MIB-Ⅰ的基础之上开发的，是 MIB-Ⅰ的一个超集。MIB-Ⅱ组被分为以下分组。

- system：关于系统的总体信息。
- interfaces：系统到子网接口的信息。
- at(address translation)：描述 Internet 到子网的地址映射。
- ip：关于系统中 IP 的实现和运行信息。
- icmp：关于系统中 ICMP 的实现和运行信息。
- tcp：关于系统中 TCP 的实现和运行信息。
- udp：关于系统中 UDP 的实现和运行信息。
- egp：关于系统中 EGP 的实现和运行信息。
- dot3(transmission)：有关每个系统接口的传输模式和访问协议的信息。
- snmp：关于系统中 SNMP 的实现和运行信息。

1) system 组

system 组提供有关被管理系统的总体信息。

2)　interfaces 组

interfaces 组包含实体物理接口的一般信息，包括配置信息和各接口中所发生事件的统计信息。

3)　address translation 组

address translation 组由一个表构成，表中的每一行对应系统中的一个物理接口，提供网络地址向物理地址的映射。一般情况下，网络地址是指系统在该接口上的 IP 地址，而物理地址决定于实际采用的子网情况。例如，如果接口对应的是 LAN，则物理地址是接口的 MAC 地址；如果对应 X.25 分组交换网，则物理地址可能是一个 X.121 地址。

实际上，address translation 组包含在 MIB-Ⅱ中只是为了与 MIB-Ⅰ兼容，MIB-Ⅱ的地址转换信息在各个网络协议组中提供。

4)　ip 组

ip 组提供了与 IP 协议有关的信息。由于端系统(主机)和中间系统(路由器)都实现了 IP 协议，而这两种系统中包含的 IP 对象又不完全相同，所以有些对象是任选的，这取决于是否与系统有关。

5)　icmp 组

icmp 是 IP 的伴随协议，所有实现 IP 协议的节点都必须实现 ICMP 协议。icmp 组包含有关 ICMP 实现和操作的有关信息，它是各种接收的或发送的 ICMP 报文的计数器。

6)　tcp 组

tcp 组包含有关一个节点的 TCP 的实现和操作的信息。

7)　udp 组

udp 组包含有关一个节点的 UDP 的实现和操作的信息。除了有关发送和接收的数据报的信息外，这个组中还包含一个 udpTable，该表中包含 UDP 端点的管理信息。UDP 端点是指正在支持本地应用接收数据报的 UDP 进程。udpTable 中包含每个 UDP 端点用户的 IP 地址和 UDP 端口。

8)　egp 组

egp 组包含有关一个节点的 EGP(External Gateway Protocol)的实现和操作的信息。除了有关发送和接收的 EGP 消息的信息外，这个组中还包含一个 egpNeighTable，该表中包含有关相邻网关的信息。

3. SNMPv2 管理信息库

SNMPv2 管理信息库扩展和细化了 MIB-Ⅱ中定义的管理对象，又增加了新的管理对象。扩展和新增的管理对象主要有以下几个。

(1)　系统组：系统组是 MIB-Ⅱ系统组的扩展。

(2)　SNMP 组：由 MIB-Ⅱ所对应的组改造而成的，有些对象被删除了，同时又增加了一些新对象。

(3)　MIB 对象组：这是一个新组，它与管理对象的控制有关。

(4)　一致性声明：是对具体实现的限制，是具体实现必须达到的最小级别。

(5)　接口组：MIB-Ⅱ定义的接口组经过一段时间的使用，发现有很多缺陷。这里的接口组是对 MIB-Ⅱ接口组的修改。

11.5.2 典型例题分析

例 11-11 在 MIB-Ⅱ中，IP 组对象 ipInReceives 为接收的数据包总数，其数据类型为类型。

A. 整数　　B. 计数器　　C. 序列　　D. 计量器

解析：在 MIB-Ⅱ中，IP 组对象 ipInReceives 为接收的数据包总数，其数据类型为计数器类型。

答案：B

例 11-12 下列说法错误的是________。

A. system 组提供有关被管系统的总体信息

B. interfaces 组包含实体物理接口的一般信息

C. address translation 组由一个表构成

D. ip 组包含有关一个节点的 TCP 的实现和操作的信息

解析：ip 组包含有关节点上 IP 的实现和操作的信息，如有关 IP 层流量的一些计数器。tcp 组包含有关一个节点的 TCP 的实现和操作的信息。

答案：D

11.5.3 同步练习

1. SNMPv2 MIB 扩展和细化了 MIB-Ⅱ中定义的管理对象，又增加了新的管理对象。扩展和新增的管理对象不包括________。

   A. 系统组　　B. SNMP 组　　C. MIB 对象组　　D. 用户组

2. SNMP MIB 中被管理对象的 Access 属性不包括_____。

   A. 只读　　B. 只写　　C. 可读写　　D. 可执行

11.5.4 同步练习参考答案

1. D　2. D

11.6 RMON

11.6.1 考点辅导

1. RMON 的基本概念

和 SNMP 同一时期还出现了用于监控局域网通信的标准——远程网络监控 RMON (Remote MONitoring)，即 RMON-1(1991)和 RMON-2(1995)。RMON 是一组定义了监视网

络通信的管理信息库的标准，是 SNMP 管理信息库的扩充，与 SNMP 配合可以提供更有效的管理性能。同时，为了适应电信网络的管理需要，ITU-T 在 1989 年定义了电信网络管理标准(Telecommunications Management Network，TMN)，即 M.30 建议。

MIB-Ⅱ能提供的只是关于单个设备的管理信息。通常把用于监视整个网络通信情况的设备称为网络监视器(Monitor)或网络分析器(Analyzer)、探测器(Probe)等。监视器观察 LAN 上出现的每个分组，并进行统计，给管理人员提供重要的管理信息。监视器还能存储部分分组，供以后分析用。监视器也根据分组类型进行过滤并捕获特殊的分组。通常是每个子网配置一个监视器，并且与中央管理站通信，因此称为远程监视器，如图 11-9 所示。图中监视器可以是一个独立设备，也可以是运行监视器软件的工作站或服务器等。中央管理站具有 RMON 管理能力，能够与各个监视器交换管理信息。RMON 监视器或探测器(RMON Probe)实现 RMON 管理信息库(RMON MIB)。这种系统与通常的 SNMP 代理一样包含一般的 MIB，另外，还有一个探测器进程，提供与 RMON 有关的功能。探测器进程能够读/写本地的 RMON 数据库，并响应管理站的查询请求。所以也把 RMON 探测器称为 RMON 代理。

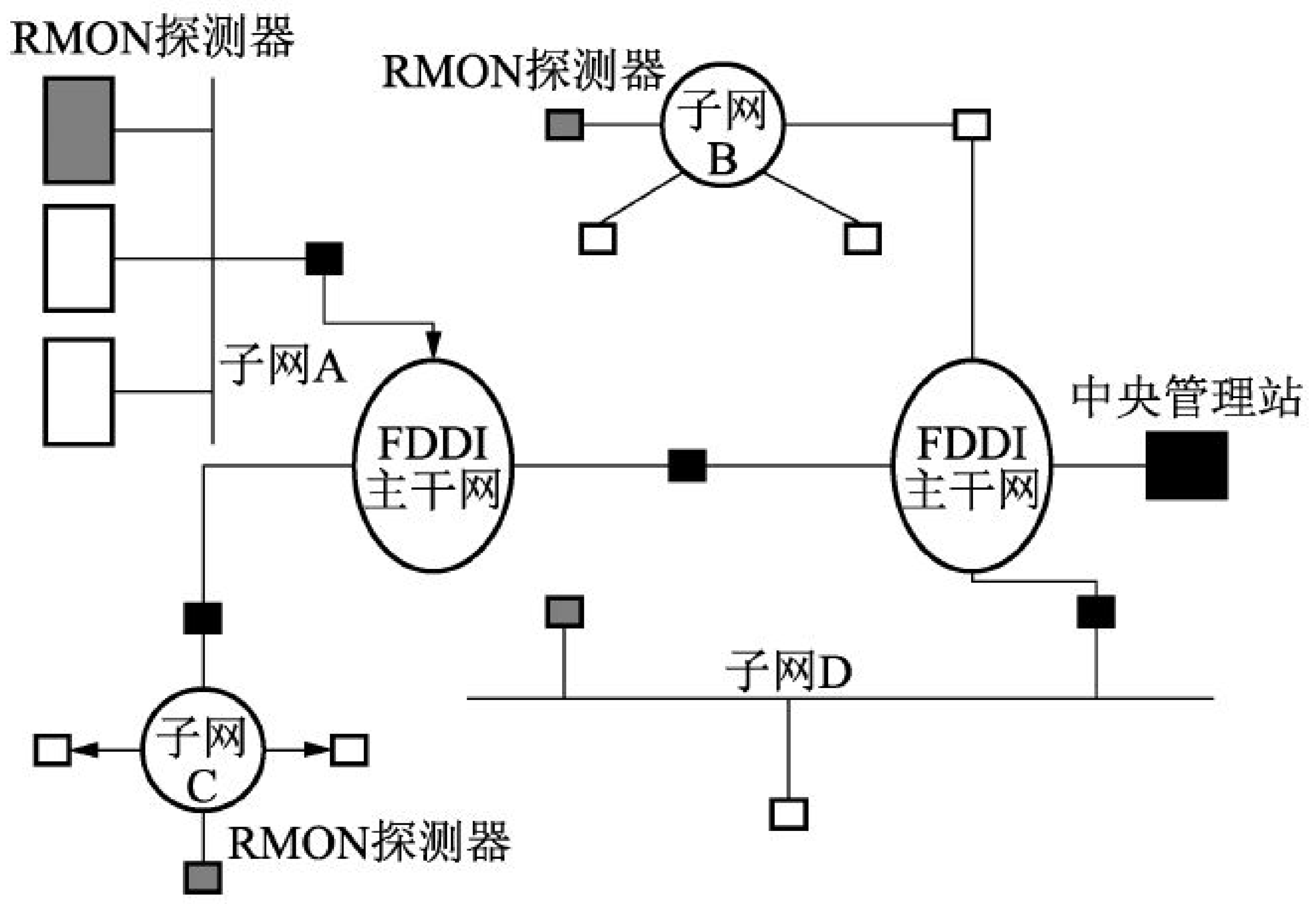


图 11-9 远程网络监视的配置

RMON 定义了远程网络监视的管理信息库，以及 SNMP 管理站与远程监视器之间的接口。

一般地说，RMON 的目标就是监视子网范围内的通信，从而减少管理站和被管理系统之间的通信负担。更具体地说，RMON 有下列目标。

- 离线操作。必要时管理站可以停止对监视器的轮询，有限的轮询可以节省网络带宽和通信费用。
- 主动监视。如果监视器有足够的资源，通信负载也允许，监视器可以连续地、周期地运行诊断程序，收集并记录网络性能参数。
- 问题检测和报告。如果主动监视消耗网络资源太多，监视器也可以被动地获取网络数据。
- 提供增值数据。监控器可以分析收集到的子网数据，从而减轻了管理站的计算任务。
- 多管理站操作。一个互联网可能有多个管理站，这样可以提高可靠性，或者分布地实现各种不同的管理功能。

在 SNMPv1 的管理框架中，对表操作的规定是很不完善的，至少增加和删除表行的操作是不明确的。RMON 规范包含一组文本约定和过程化规则，在不修改、不违反 SNMP 管理框架的前提下提供了明晰而规律的行增加和行删除操作。

2. RMON 的管理信息库

RMON 规范定义了 RMON 管理信息库 RMON MIB，它是 MIB-Ⅱ下面的第十六个子树。RMON MIB 分为 10 组，如图 11-10 所示。存储在每一组中的信息都是监视器从一个或几个子网中统计和收集的数据。这 10 个功能组都是任选的，但实现时有下列连带关系。

- 实现警报组时必须实现事件组。
- 实现最高 *N* 台主机组时必须实现主机组。
- 实现捕获组时必须实现过滤组。

RMON(MIB-Ⅱ16)
- Statistics(1)以太网的统计信息
- History(2)子网的周期性统计信息
- Alarm(3)用于定义取样间隔和报警阈值
- Host(4)关于一个主机的通信统计数据
- Host Top*N*(5)某种参数量大的*N*台主机的统计数据
- Matrix(6)一对地址之间的通信统计数据
- Filter(7)对分组进行过滤的信息
- Capture(8)捕获特殊分组的信息
- Event(9)定义网络事件的信息
- TokenRing(10)关于令牌环网的配置和统计信息

图 11-10　RMON MIB 子树

这 10 个功能组的功能说明如下。

1)　统计组

统计组(Statistics)统计被监控的每个子网的基本统计信息。网络管理员可以从 RMON 探针监测的设备端口获取一个网段的各种统计信息。目前只能对网络设备的以太网接口进行监控和统计，将来会扩展到包括更多接口的特定表格(如 FDDI)。它能统计一个网段的流量(如交通流量的总包数和总字节数)，统计各种类型包的分布(如广播包、多点广播包、不同大小包的数量)，还能统计各种类型错误包数、碰撞次数等。

2)　历史组

历史组(History)定期地收集统计网络值的记录并存储起来，方便日后的处理。它包含历史控制组和以太网历史组两个小组。其中，历史控制组主要用来设置采样间隔时间等控制信息；以太网历史组为网络管理员提供有关网段流量、错误包、广播包、利用率及碰撞次数等其他统计信息的历史数据。

3)　警报组

警报组(Alarm)允许网络管理站为网络性能(可以是监视器本地 MIB 的任意整数类型的对象)定义一组报警阈值。如果阈值在相应的方向上被越过，监视器就会产生警报并把警报发往网络管理站。警报组需要事件组的实现。

4)　主机组

主机组(Host)包含对连接在一个子网上所有主机的各种类型统计的计数值。它能够发现

网上的新主机，对每个主机的 MAC 地址保持一组统计数据，如主机发送或接收的数据包总数、广播包数、流量字节数和错误包数等。它有一个控制表和两个数据表，且这两个数据表的内容相同，只是组织排列顺序不同。

5) 最高主机组

最高主机组(Host Top*N*)包括排序后的主机统计，该报告基于主机表中的一些参数生成列表。它用于统计在一个子网上一些参数最高的一组主机，如它可以列出 10 个传输数据最多的主机，但依赖于主机组的实现。

6) 矩阵组

矩阵组(Matrix)用于记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储。这种方法对于检索特定主机之间的流量信息十分有用，如用于找出哪些设备对服务器的使用最多。矩阵组由 3 个表组成，即一个控制表加上两个数据表。

7) 过滤组

过滤组(Filter)允许监视器观测与过滤器相匹配的数据包。网络监视器可以捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。

8) 包捕获组

包捕获组(Capture)控制数据被发往网管站的方式，它可以在把报文发送到某个通道后记录数据报文。

9) 事件组

事件组(Event)提供关于 RMON 代理所产生的所有事件的列表。当某事件发生时可以记录日志和发送 IRAP 到网管站。

10) 令牌环网组

RFC1513 扩展了 RMON MIB，增加了有关 IEEE 802.5 令牌环网的管理信息。首先是在统计组增加了两个表，即 tokenRingMLStatsTable 和 tokenRingPStatsTable，前者统计令牌环中各种 MAC 控制分组，后者统计各种数据分组。根据 RFC1757 的定义，好的分组就是没有错误并具有有效长度的分组；坏的分组是帧格式可以识别，但是含有错误，或者具有无效长度的分组。

3. RMON2 的管理信息库

尽管 RMON 有很多优点，但也有其局限性。RMON 的 MAC 层探测器不能确定由服务器进入本地网段的数据包的源点和终点，或者是不能确定经过被监视网段的通信数据包的源点和终点。

1994 年，RMON2 工作组开始致力于提高现存的物理层和数据链路层之间的 RMON 规范，以实现在网络层和应用层提供历史和数据的统计服务。

在网络层，RMON2 通过监视点对点通信来记录网络使用的模式。另外，RMON2 还显示单个应用所占用的带宽，以及出现疑难故障的关键因素。

RMON2 监视 OSI/RM 第三至七层的通信，能对数据链路层以上的分组进行译码。这使得监视器可以管理包括 IP 等网络层协议。因而能了解分组的源和目标地址，能知道路由器负载的来源，使得监视的范围扩大到局域网外。监视器也能监视应用层协议，如电子邮件协议、文件传输协议、HTTP 等，这样监视器就可以记录主机应用活动的数据，可以显示

各种应用活动的图表。这些对网络管理人员都是很重要的信息。另外，在网络管理标准中，通常把网络层上的协议都称为应用层协议，以后提到的应用层包含 OSI 的第五至七层。

RMON2 扩充了原来的 RMON MIB，增加了 9 个新的功能组，如图 11-11 所示。

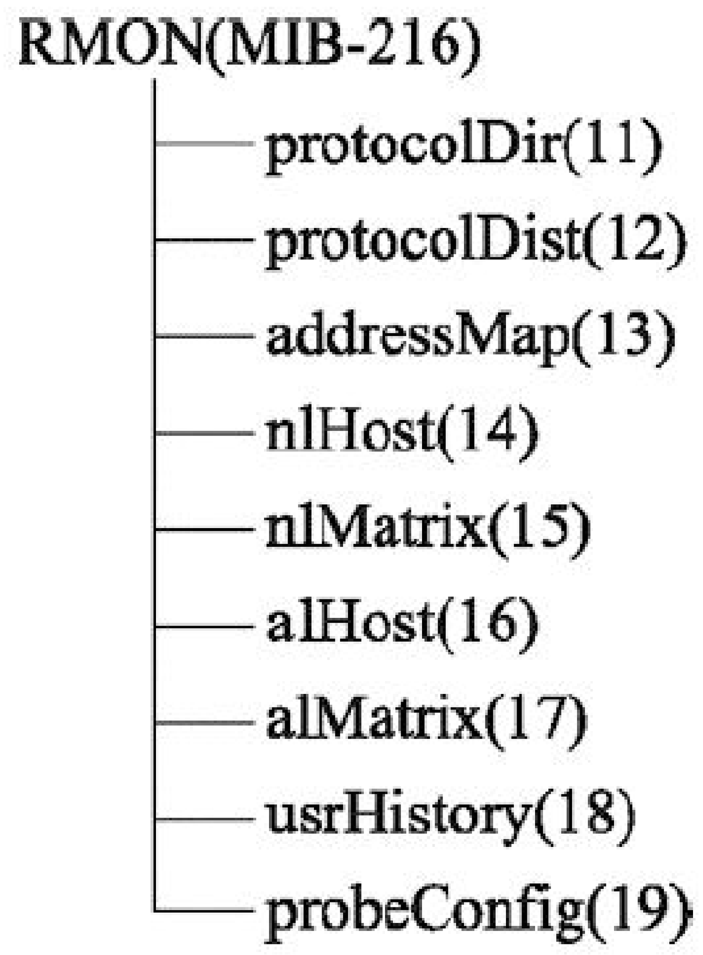


图 11-11　RMON2 MIB

下面对这 9 个新功能组进行说明。

协议目录组(protocolDir)：提供了表示各种网络协议的标准化方法，使得管理站可以了解监视器所在的子网上运行什么协议。

协议分布组(protocolDist)：提供每个协议产生的通信统计数据。

地址映像组(addressMap)：建立网络层地址(IP 地址)与 MAC 地址的映像关系。这些信息在发现网络设备、建立网络拓扑结构时有用。

网络层主机组(nlHost)：类似于 RMON1 的主机组，收集网上主机的信息。但是与 RMON1 不同，这一组不是基于 MAC 地址，而是基于网络层地址发现主机。这样管理人员可以超越路由器看到子网之外的 IP 主机。

网络层矩阵组(nlMatrix)：记录主机对(源/目标)之间的通信情况，收集的信息类似于 RMON1 的矩阵组，但是按网络层地址标识主机。

应用层主机组(alHost)：对应每个主机的每个应用协议(指第三层之上的协议)在 alHost 表中有一个表项，记录有关主机发送/接收的分组/字节数等。这一组使用户可以了解每个主机上的每个应用协议的通信情况。

应用层矩阵组(alMatrix)：统计一对应用层协议之间的各种通信情况，以及某种选定的参数(如交换的分组数/字节数)最大的(Top*N*)一对应用层协议之间的通信情况。

用户历史组(usrHistory)：按照用户定义的参数，周期性地收集统计数据。这使得用户可以研究系统中的任何计数器。

监视器配置组(probeConfig)：定义了监视器的标准参数集合，这样可以提高管理站和监视器之间的互操作性，使得管理站可以远程配置不同制造商的监视器。

11.6.2　典型例题分析

例 11-13　管理站用 SetRequest 在 RMON 表中产生一个新行，如果新行的索引值与表中其他行的索引值不冲突，则代理产生一个新行，其状态对象的值为<u>　(47)　</u>。(2014 年上半年真题 47)

A. creatRequest　　B. underCreate　　C. valid　　D. invalid

解析：本题考查 RMON 的基本知识。

管理站用 Set 命令在 RMON 表中增加新行，遵循的规则是：管理站用 SetRequest 在 RMON 表中产生一个新行，如果新行的索引值与表中其他行的索引值不冲突，则代理产生一个新行，其状态对象的值为 createRequest。

答案：A

11.6.3　同步练习

RMON 和 SNMP 的主要区别是______。

A. RMON 只能提供单个设备的管理信息，而 SNMP 可以提供整个子网的管理信息

B. RMON 提供了整个子网的管理信息，而 SNMP 管理信息库只包含本地设备的管理信息

C. RMON 定义了远程网络的管理信息库，而 SNMP 只能提供本地网络的管理信息

D. RMON 只能提供本地网络的管理信息，而 SNMP 定义了远程网络的管理信息库

11.6.4　同步练习参考答案

B

11.7　网络诊断和配置命令

11.7.1　考点辅导

1. ipconfig

ipconfig 工具用来显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议(DHCP)和域名系统(DNS)设置。使用不带参数的 ipconfig 可以显示所有适配器的 IP 地址、子网掩码、默认网关。

1)　语法格式

```
ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns]
[/displaydns] [/registerdns] [/showclassid Adapter] [/setclassid Adapter
[ClassID]]
```

2)　参数说明

参数如表 11-1 所示。

表 11-1　ipconfig 的选项

选　项	描　述
/all	显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下，只显示 IP 地址、子网掩码和各个适配器的默认网关值
/renew [*adapter*]	更新所有适配器或特定适配器的 DHCP 配置。仅在具有配置为自动获取 IP 地址的网卡的计算机上可用
/release [*adapter*]	发送 DHCPRELEASE 消息到 DHCP 服务器，以释放所有适配器或特定适配器的当前 DHCP 配置并丢弃 IP 地址配置。同样仅在具有配置为自动获取 IP 地址的网卡的计算机上可用
/flushdns	清理并重设 DNS 客户解析器缓存的内容
/displaydns	显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录以及由计算机解析的名称查询而最近获得的任何资源记录

续表

选　项	描　述
/registerdns	初始化计算机上配置的 DNS 名称和 IP 地址的手工动态注册
/showclassid *Adapter*	显示指定适配器的 DHCP 类别 ID
/setclassid *Adapter* [*ClassID*]	配置特定适配器的 DHCP 类别 ID
/?	在命令提示符下显示帮助

3) 注释

ipconfig 等价于 winipcfg，后者在 Windows Millennium Edition、Windows 98 和 Windows 95 上可用。

2. ping

ping 通过发送“Internet 控制报文协议(ICMP)”回送请求/应答报文来验证与另一台 TCP/IP 计算机的 IP 级连接。回送请求/应答报文的接收情况将和往返过程的次数一起显示出来。ping 是用于检测网络连接性、可到达性和名称解析的疑难问题的主要 TCP/IP 命令。如果不带参数，ping 将显示帮助。

1) 语法格式

```
ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count] [-s
Count] [{-j HostList | -k HostList}] [-w Timeout] [TargetName]
```

2) 参数说明

参数如表 11-2 所示。

表 11-2　ping 的选项

选　项	描　述
-t	中断前持续发送回响请求信息到目的地，按 Ctrl+Break 组合键中断并显示统计信息，按 Ctrl+C 组合键中断并退出
-a	对目的地 IP 地址进行反向名称解析，若解析成功，将显示相应的主机名
-n *Count*	指定发送回响请求消息的次数。默认值为 4
-l *Size*	指定发送消息中“数据”字段的长度。默认值为 32B，最大值是 65527B
-f	指定发送的回响请求消息带有“不要拆分”标志，用于检测并解决“路径最大传输单位(PMTU)”的故障
-i *TTL*	指定发送回响请求消息的 IP 标题中的 TTL 字段值。其默认值是主机的默认 TTL 值。对于 Windows XP 主机，该值一般是 128。TTL 的最大值是 255
-v *TOS*	指定发送回响请求消息的 IP 标题中的“服务类型(TOS)”字段值。默认值是 0。TOS 被指定为 0～255 的十进制数
-r *Count*	指定 IP 标题中的“记录路由”选项，用于记录由回响请求消息和相应的回响应答消息使用的路径。最小值必须为 1，最大值为 9
-s *Count*	指定 IP 标题中的“Internet 时间戳”选项，用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。最小值为 1，最大值为 4

续表

选　项	描　述
-k *HostList*	在 IP 头中使用严格源路由选项，HostList 指明中间节点(路由器)的地址或名字。最多 9 个，用空格分开
-w *Timeout*	指定等待回响应答消息响应的时间(ms)，默认的超时时间为 4000ms
TargetName	指定目的端，它既可以是 IP 地址，也可以是主机名

3. arp

arp 命令用于显示和修改 ARP 缓存中的项目。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。如果在没有参数的情况下使用，则 arp 命令将显示帮助信息。

1) 语法格式

```
arp [-a [inet_addr] [-N if_addr]] [-g [inet_addr] [-N if_addr]] [-d inet_addr
[if_addr]] [-s inet_addr eth_addr [if_addr]]
```

2) 参数说明

- -a [inet_addr] [-N if_addr]：显示所有接口的当前 ARP 缓存表。要显示特定 IP 地址的 ARP 缓存项，请使用带有 inet_addr 参数的 arp -a 命令，此处的 inet_addr 代表 IP 地址。如果未指定 inet_addr，则使用第一个适用的接口。要显示特定接口的 ARP 缓存表，请将-N if_addr 参数与-a 参数一起使用，此处的 if_addr 代表指派给该接口的 IP 地址。-N 参数区分大小写。
- -g [inet_addr] [-N if_addr]：与-a 相同。
- -d inet_addr [if_addr]：删除指定的 IP 地址项，inet_addr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 if_addr 参数。
- -s inet_addr eth_addr [if_addr]：向 ARP 缓存添加可将 IP 地址 inet_addr 解析成物理地址 eth_addr 的静态项。要向指定接口的表添加静态 ARP 缓存项，使用 if_addr 参数。

4. netstat

netstat 工具可用来显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP)及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 及通过 IPv6 的 UDP)。使用时如果不带参数，netstat 显示活动的 TCP 连接。

1) 语法格式

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```

2) 参数说明

参数介绍如表 11-3 所示。

表 11-3　netstat 的选项

选　项	描　述
-a	显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口
-e	显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与 -s 结合使用
-n	显示活动的 TCP 连接，不过只以数字形式表现地址和端口号，却不尝试确定名称
-o	显示活动的 TCP 连接并包括每个连接的进程 ID(PID)，可以与 -a、-n 和 -p 结合使用
-p Protocol	显示 protocol 所指定协议的连接。在这种情况下，protocol 可以是 tcp、udp、tcpv6 或 udpv6。如果该参数与-s 一起使用，按协议显示统计信息，则 protocol 可以是 tcp、udp、icmp、ip、tcpv6、udpv6、icmpv6 或 ipv6
-s	按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计信息。若安装了 IPv6，就会显示有关 IPv6 上的 TCP、IPv6 上的 UDP、ICMPv6 和 IPv6 的统计信息。可以使用-p 参数指定协议集
-r	显示 IP 路由表的内容。该参数与 route print 命令等价
interval	每隔 Interval 秒重新显示一次选定的信息。按 Ctrl+C 组合键停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息

5. tracert

tracert 通过递增“生存时间(TTL)”字段的值“Internet 控制报文协议(ICMP)”回送请求/应答报文发送给目标可确定到达目标的路径。所显示的路径是源主机与目标主机间的路径中的路由器的近侧路由器接口列表。近侧接口是距离路径中的发送主机最近的路由器的接口。不带参数时，tracert 显示帮助。

1)　语法格式

```
tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]
```

2)　参数说明

- /d：防止 tracert 试图将中间路由器的 IP 地址解析为它们的名称。
- -h MaximumHops：在搜索目标(目的)的路径中指定跃点的最大数。默认值为 30 个跃点。
- -j HostList：说明发送回声请求报文要使用 IP 头中的松散源路由选项，标识符 HostList 列出必须经过的中间节点的地址或名字，最多可以列出 9 个中间节点，各个中间节点用空格隔开。
- -w Timeout：说明了等待 ICMP 回声响应报文的时间(μs)，如果接收超时，则显示星号“*”，默认超时间隔是 4s。
- TargetName：指定目标，可以是 IP 地址或主机名。

6. pathping

pathping 是一个将 ping 和 tracert 的功能结合起来并有所增强的网络诊断工具，它可以反映出数据包从源主机到目标主机所经过的路径、网络延时及丢包率，帮助用户解决网络问题。

1)　语法格式

```
pathping [-n] [-h maximum_hops] [-g host-list] [-p period] [-q num_queries]
[-w timeout] [-i address] [-R] [-T] [-4] [-6] target_name
```

2)　参数说明

参数介绍如表 11-4 所示。

表 11-4　pathping 的选项

选　项	描　述
-n	阻止 pathping 试图将中间路由器的 IP 地址解析为各自的名称
-h maximum_hops	指定搜索目标(目的)的路径中存在的跃点的最大数。默认值为 30 个跃点
-g host-list	指定回响请求消息利用 host-list 中指定的中间目标集在 IP 数据头中使用"稀疏来源路由"选项。host-list 中的地址或名称的最大数为 9
-p period	指定两个连续的 ping 之间的时间间隔(以 ms 为单位)。默认值为 250ms(即 1/4s)
-q num_queries	指定发送到路径中每个路由器的回响请求消息数。默认值为 100 个查询
-w timeout	指定等待每个应答的时间(以 ms 为单位)。默认值为 3000ms(即 3s)
-i address	指定源地址
-R	检查以确定路径中的每个路由器是否支持"资源保留协议(RSVP)"
-T	将 2 级优先级标记(如对于 IEEE 802.1p)连接到数据包并将它发送到路径中的每个网络设备
-4	指定 pathping 只使用 IPv4
-6	指定 pathping 只使用 IPv6
target_name	指定目的端，它既可以是 IP 地址，也可以是主机名

7. nbtstat

nbtstat 命令是 Windows 下自带的 NetBIOS 管理工具，用于显示本地计算机和远程计算机的基于 TCP/IP 的 NetBIOS 统计资料、本地计算机和远程计算机的 NetBIOS 名称表和 NetBIOS 名称缓存。nbtstat 可以刷新 NetBIOS 名称缓存和使用 Windows Internet 名称服务(WINS)注册的名称。使用不带参数的 nbtstat 则显示帮助信息。

1)　语法格式

```
nbtstat [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S]
[interval]
```

2)　参数说明

nbtstat 参数介绍如表 11-5 所示。

表 11-5　nbtstat 的选项

选　项	描　述
-a RemoteName	显示远程计算机的名称，并列出其名称列表。其中，RemoteName 是远程计算机的 NetBIOS 名称
-A IP address	显示远程计算机的 NetBIOS 名称表，其名称由远程计算机的 IP 地址指定。和-a 不同的是这个只能使用 IP，其实-a 就包括了-A 的功能了

续表

选　项	描　述
-c	显示远程计算机 NetBIOS 名称的缓存和每个名称的 IP 地址，此参数用来列出 NetBIOS 里缓存连接过的计算机的 IP
-n	显示本地计算机的 NetBIOS 名称表。Registered 的状态表明该名称是通过广播还是 WINS 服务器注册的
-r	显示 NetBIOS 名称解析统计资料。在配置为使用 WINS 且运行 Windows XP 或 Windows Server 2003 操作系统的计算机上，该参数将返回已通过广播和 WINS 解析和注册的名称号码
-R	清除 NetBIOS 名称缓存的内容并从 Lmhosts 文件中重新加载带有#PRE 标记的项目
-RR	释放并刷新通过 WINS 服务器注册的本地计算机的 NetBIOS 名称
-s	显示 NetBIOS 客户端和服务器会话，并将目标 IP 地址转化为名称
-S	显示 NetBIOS 客户端和服务器会话，只通过 IP 地址列出远程计算机
interval	每隔 interval 秒重新显示选择的统计资料，按 Ctrl+C 组合键停止重新显示统计信息。如果省略该参数，nbtstat 将只显示一次当前的配置信息

注：NetBIOS 名称表是与运行在该计算机上的应用程序相对应的 NetBIOS 名称列表。

8. route

route 命令的功能是显示和修改本地的 IP 路由表。如果不带参数，则给出帮助信息。

1) 语法格式

```
route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric
Metric] [if Interface]]
```

2) 参数说明

- -f：删除路由表中的网络路由、本地环路路由和组播路由。
- -p：与 add 命令联合使用时，一条路由被添加到注册表中，当 TCP/IP 启动时，用于初始化路由；与 print 命令联合使用时，则显示持久路由列表；对于其他命令，这个参数被忽略。
- Command：表示要运行的命令，可用的命令有 add(添加路由)、change(修改已有的路由)、delete(删除路由)和 print(打印路由)。
- Destination：说明目标地址，可以是网络地址、主机地址或默认路由。
- mask Netmask：说明目标地址对应的子网掩码。
- Gateway：说明下一跃点的 IP 地址。
- metric Metric：说明路由度量值，通常选择度量值最小的路由。
- if Interface：说明接口的索引。

9. netsh

netsh 是一个命令行脚本实用程序，可用于修改计算机的网络配置。

利用 netsh 也可以建立批文件来运行一组命令，或者把当前的配置脚本用文本文件保存起来，以后可用来配置其他的服务器。

1)　netsh 上下文

netsh 利用动态链接库与操作系统的其他组件交互作用。netsh 助手是一个动态链接库文件，提供了称为上下文的扩展特性，可以对多种服务、实用程序或协议提供配置和监视功能。从一个上下文可以转到另一个上下文，后者称为子上下文。

2)　在 Cmd.exe 命令提示符下运行 netsh 命令

为了在远程 Windows Server 2003 中运行 netsh 命令，首先要通过“远程桌面连接”连接到正在运行终端服务器的 Windows Server 2003 系统中。在 Cmd.exe 命令提示符下输入 netsh，就进入了 netsh>提示符。netsh 的语法格式如下。

```
netsh [-a AliasFile] [-c Context] [-r RemoteComputer] [{NetshCommand |-f
ScriptFile}]
```

参数说明如下。

- -a AliasFile：运行 AliasFile 文件后返回 netsh 提示符。
- -c Context：转到特定的 netsh 上下文。
- -r RemoteComputer：配置远程计算机。
- NetshCommand：说明要使用的 netsh 命令。
- -f ScriptFile：运行脚本后转出 netsh.exe。

10. nslookup

nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令工具。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。

1)　语法格式

```
nslookup [-SubCommand...] [{ComputerToFind | -Server}]
```

2)　参数说明

- -SubCommand...：将一个或多个 nslookup 子命令指定为命令行选项。
- ComputerToFind：如果未指定其他服务器，就使用当前默认 DNS 名称服务器查阅 ComputerToFind 的信息。要查找不在当前 DNS 域的计算机，请在名称上附加句点。
- -Server：指定将该服务器作为 DNS 名称服务器使用。如果省略了-Server，将使用默认的 DNS 名称服务器。

3)　nslookup 的两种模式

nslookup 有两种模式，即交互式和非交互式。

如果仅需要查找一块数据，请使用非交互式模式。对于第一个参数，输入要查找的计算机的名称或 IP 地址。对于第二个参数，输入 DNS 名称服务器的名称或 IP 地址。如果省略第二个参数，nslookup 使用默认 DNS 名称服务器。

如果需要查找多块数据，可以使用交互模式。第一个参数输入连字符(-)，第二个参数输入 DNS 名称服务器的名称或 IP 地址。或者，省略两个参数，则 nslookup 使用默认 DNS 名称服务器。在交互方式下，可以用 set 命令设置选项，以满足指定的查询需要。

- >set all：列出当前设置的默认选项。

- set type=mx：查询本地域的邮件交换器信息。
- server NAME：由当前默认服务器切换到指定的名字服务器 NAME。
- ls：用于区域传输，罗列出本地区域中的所有主机信息。
- set type：设置查询的资源记录类型。DNS 服务器主要的资源记录有 A(域名到 IP 地址的映射)、PTR(IP 地址到域名的映射)、MX(邮件服务器及其优先级)、CNAM(别名)和 NS(区域的授权服务器)等类型。
- set type=any：对查询的域名显示各种可用的信息资源记录(A、CNAME、MX、NS、PTR、SOA 和 SRV 等)。
- set debug：显示查询过程的详细信息，这些信息可用于对 DNS 服务器进行排错。

11. net

在网络管理中，最为常用的就是 net 命令家族。常用的 net 命令有以下几个。

- net view 命令：显示由指定的计算机共享的域、计算机或资源的列表。
- net share：用于管理共享资源，使网络用户可以使用某一服务器上的资源。
- net use 命令：用于将计算机与共享的资源相连接或断开，或者显示关于计算机连接的信息。
- net start 命令：用于启动服务，或显示已启动服务的列表。
- net stop 命令：用于停止正在运行的服务。
- net user 命令：可用来添加或修改计算机上的用户账户，或者显示用户账户的信息。
- net config 命令：显示正在运行的可配置服务，或显示和更改服务器服务或工作站服务的设置。
- net send 命令：用于将消息(可以是中文)发送到网络上的其他用户、计算机或者消息名称上。
- net localgroup 命令：用于添加、显示或修改本地组。
- net accounts 命令：可用来更新用户账户数据库、更改密码及所有账户的登录要求。

11.7.2　典型例题分析

例 11-14　在 Windows 中，以下命令运行结果中不出现网关 IP 地址的是 __(59)__ 。(2017 年下半年真题 59)

A. arp　　B.ipconfig　　C.netstat　　D.tracert

解析：arp 虽然可以看到网关的 IP 和 Mac，但不一定是网关地址。

答案：A

例 11-15　某网络管理员在网络检测时，执行了 undomac-addressblackhole 命令。该命令的作用是 __(46)__ 。(2017 年上半年真题 46)

A. 禁止用户接口透传 VLAN　　B. 关闭接口的 MAC 的学习功能

C. 为用户接口配置了端口安全　　D. 删除配置的黑洞 MAC

解析：blackhole：目的黑洞 MAC 地址表项，当报文的目的 MAC 地址与目的黑洞 MAC 地址表项匹配后该报文被丢弃，undomac-addressblackhole 的含义就是撤销 MAC 地址的

黑洞。

答案：D

例 11-16 在发现主机受到 ARP 攻击时需清除 ARP 缓存，使用的命令是 (48) 。(2016 年下半年真题 48)

A. arp -a　　B. arp -s　　C. arp -d　　D. arp -g

解析：arp -a:显示所有接口的 ARP 缓存表。

arp -s:添加一个静态的 ARP 表项。

arp -d:删除 ARP 缓存表项。

arp -g:与 arp -a 相同。

答案：C

例 11-17 客户端采用 ping 命令检测网络连接故障时，可以 ping 通 127.0.0.1 及本机的 IP 地址，但无法 ping 通同一网段内其他工作正常的计算机的 IP 地址。该客户端的故障可能是 (49) 。(2016 年上半年真题 49)

A. TCP/IP 不能正常工作　　B. 本机网卡不能正常工作

C. 网络线路故障　　D. 本机 DNS 服务器地址设置错误

解析：可以 ping 通 127.0.0.1 及本机的 IP 地址，证明 TCP/IP、网卡均能正常工作；无法 ping 通同一网段内其他工作正常的计算机的 IP 地址，该故障和本机 DNS 服务器地址设置无关，故推断为网络线路故障。

答案：C

例 11-18 使用 tracert 命令进行网络检测，结果如下图所示，那么本地默认网关地址是 (64) 。(2016 年上半年真题 64)

```
C:\>tracert 110.150.0.66
Tracing route to 110.150.0.66 over a maximum of 30 hops
1 2s 3s 2s 10.10.0.1
2 75ms 80ms 100ms 192.168.0.1
3 77ms 87ms 54ms 110.150.0.66
Trace complete
```

A. 110.150. 0.66　　B. 101.10.0.1

C. 192.168. 0.1　　D. 127.0.0.1

解析：tracert 是路由跟踪命令，用于确定 IP 数据包访问目标所采取的路径。根据题意，第一条就是本地网关返回的信息，那么本地默认网关就是 101.10.0.1。

答案：B

例 11-19 在 Windows 客户端运行 nslookup 命令，结果如下图所示。为 www.softwaretest.com 提供解析的是 (33) 。在 DNS 服务器中，ftp.softwaretest.com 记录通过 (34) 方式建立。(2015 年下半年真题 33、34)

```
C:\Documents and Settings\user>nslookup  www.softwaretest.com
Server:   ns1.softwaretest.com
Address: 192.168.1.254

Non-authoritative answer:
Name:    www.softwaretest.com
Address: 10.10.1.3

C:\Documents and Settings\user>nslookup  ftp.softwaretest.com
Server:   ns1.softwaretest.com
Address: 192.168.1.254

Non-authoritative answer:
Name:    ns1.softwaretest.com
Address:  10.10.1.1
Aliases:  ftp.softwaretest.com
```

(33) A. 192.168.1.254　　B. 10.10.1.3
　　C. 10.10.1.1　　D. 192.168.1.1

(34) A. 主机　　B. 别名　　C. 邮件交换器　　D. PIR 记录

解析：DNS 资源记录如下。

SOA 记录：SOA 说明能解析这个区域的 DNS 服务器中哪个是主服务器。

NS 记录：用于标识区域的 DNS 服务器有几台提供服务。

A 记录：也称为主机记录，是 DNS 名称到 IP 地址的映射，用于正向解析。

PTR 记录：是 IP 地址到 DNS 名称的映射，用于反向解析。

MX 记录：邮件交换记录。在使用邮件服务器的时候，MX 记录是不可或缺的，比如 A 用户向 B 用户发送一封邮件，那么他需要向 DNS 查询 B 的 MX 记录，DNS 在定位到了 B 的 MX 记录后反馈给 A 用户，然后 A 用户把邮件投递到 B 用户的 MX 记录邮件服务器中。

CNAME 记录：别名记录，这种记录允许用户将多个域名映射到同一台计算机。通常用于同时提供多种应用服务的计算机。例如，有一台计算机名为“host.csai.cn”(A 记录)，它同时提供 WWW 和 FTP 服务，为了便于用户访问服务，可以为该计算机设置两个别名(CNAME)：WWW 和 FTP。这两个别名的全称就是“www.csai.cn”和“ftp.csai.cn”。实际上它们都指向同一台计算机。

A 记录就是把一个域名解析到一个 IP 地址，而 CNAME 记录就是把域名解析到另外一个域名，其功能差不多。CNAME 将几个主机名指向一个别名，其实跟指向 IP 地址是一样的，因为这个别名也要做一个 A 记录的。但是使用 CNAME 记录可以很方便地变更 IP 地址。如果一台服务器有 100 个网站，它们都做了别名，该台服务器变更 IP 时，只需要变更别名的 A 记录就可以了。

答案：(33) A　(34) B

例 11-20　根据下图所示的输出信息，可以确定的是__(46)__。(2015 年下半年真题 46)

```
C:\> netstat –n

Active Connections

Proto    Local Address         Foreign Address        State
TCP      192.168.0.200:2011    202.100.112.12:443     ESTABLISHED
TCP      192.168.0.200:2038    100.29.200.110:110     TIME_WAIT
TCP      192.168.0.200:2052    128.105.129.30:80      ESTABLISHED
```

A. 本地主机正在使用的端口号是公共端口号

B. 192.168.0.200 正在与 128.105.129.30 建立连接

C. 本地主机与 202.100.112.12 建立了安全连接

D. 本地主机正在与 100.29.200.110 建立连接

解析：netstat - n 命令用于显示所有已建立的有效连接。连接状态如下。

LISTEN：侦听来自远方的 TCP 端口的连接请求。

SYN-SENT：在发送连接请求后等待匹配的连接请求。

SYN-RECEIVED：在收到和发送一个连接请求后等待对方对连接请求的确认。

ESTABLISHED：代表一个打开的连接。

FIN-WAIT-1：等待远程 TCP 连接中断请求，或对先前的连接中断请求的确认。

FIN-WAIT-2：从远程 TCP 等待连接中断请求。

CLOSE-WAIT：等待从本地用户发来的连接中断请求。

CLOSING：等待远程 TCP 对连接中断的确认。

LAST-ACK：等待对原来的发向远程 TCP 的连接中断请求的确认。

TIME-WAIT：等待足够的时间以确保远程 TCP 接收到对连接中断请求的确认。

CLOSED：没有任何连接状态。

本机使用 3 个不同的端口号，通过 2011 端口与 202.100.112.12 建立了安全连接，通过 2052 端口与 128.105.129.30 建立了安全连接，通过 2038 端口与 100.29.200.110 进行连接中断。

答案： C

例 11-21　查看 DNS 缓存记录的命令是__(34)__。(2015 年上半年真题 34)

A. ipconfig/flushdns　　　　B. nslookup

C. ipconfig/release　　　　D. ipconfig/displaydns

解析：ipconfig/flushdns 用于刷新客户端 DNS 缓存的内容；ipconfig/release 用于向 DHCP 服务器发送 DHCP Release 请求，释放网卡的 DHCP 配置参数和当前使用的 IP 地址；ipconfig/displaydns 用于显示客户端 DNS 缓存的内容；nsloopup 用于显示 DNS 查询信息，诊断和排除 DNS 故障。

答案：D

例 11-22　一台主机的浏览器无法访问域名为 www.sohu.com 的网站，并且在这台计算机执行 tracert 命令时有如下信息。

```
Tracing router to www.sohu.com [202.113.96.10] Over maximum of 30 hops:
1  <1ms  <1ms  1ms  59.67.148.1
2  59.67.148.1  reports: Destination net unreachable
Trace complete
```

根据以上信息，造成这种现象的原因可能是__(47)__。(2015 年上半年真题 47)

A. 该计算机 IP 地址设置有误　　B. 相关路由器上进行了访问控制

C. 本地网关不可达　　D. 本地 DNS 服务器工作不正常

解析：从图中可看出 www.sohu.com 已经成功解析，可得出 IP 地址没问题，网关以及 DNS 正常工作。由提示 Destination net unreachable(无法到达目标网络)可知，问题应出在路由器上。

答案： B

例 11-23　使用 netstat-o 命令可显示网络__(48)__。(2015 年上半年真题 48)

A. IP、ICMP、TCP、UDP 的统计信息

B. 以太网统计信息

C. 以数字格式显示所有连接、地址及端口

D. 每个连接的进程 ID

解析：本题考查网络管理命令 netstat 的使用及相关参数的作用。

netstat 命令用于显示 TCP 连接。Netstat 命令的语法如下：

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```

对以上参数解释如下。

-a：显示所有活动的 TCP 连接，以及正在监听的 TCP 和 UDP 端口。

-e：显示以太网统计信息，例如发送和接收的字节数，以及出错的次数等。这个参数可以与-s 参数联合使用。

-n：显示活动的 TCP 连接，地址和端口号以数字形式表示。

-o：显示活动的 TCP 连接以及每个连接对应的进程 ID。在 Windows 任务管理器中可以找到与进程 ID 对应的应用。这个参数可以与-a、-n 和-p 联合使用。

-p Protocol：用标识符 Protocol 指定要显示的协议，可以是 TCP、UDP、TCPv6 或者 UDPv6。如果与参数-s 联合使用，则可以显示协议 TCP、UDP、ICMP、IP、TCPv6、UDPv6，ICMPv6 或 IPv6 的统计数据。

-s：显示每个协议的统计数据。默认情况下，统计 TCP、UDP、ICMP 和 IP 协议发送和接收的数据包、出错的数据包、连接成功或失败的次数等。如果与-p 参数联合使用，可以指定要显示统计数据的协议。

-r：显示 IP 路由表的内容，其作用等价于路由打印命令 route printo。

Interval：说明重新显示信息的时间间隔，按 Ctrl+C 组合键则停止显示。如果不使用这个参数，则只显示一次。

答案：D

例 11-24　如果要检查本机的 IP 是否工作正常，则应该 ping 的地址是__(53)__。(2015 年上半年真题 53)

A. 192.168.0.1　　　B. 10.1.1.1　　　C. 127.0.0.1　　　D. 128.0.1.1

解析：127.0.0.1 是一个回送地址，指本地机，一般用 ping 127.0.0.1 来测试本地 TCP/IP 是否正常，如能 ping 通则说明正常。

答案：C

11.7.3 同步练习

1. 在 Windows 命令行窗口中输入 tracert 命令，得到下图所示窗口，则 PC 的 IP 地址可能为________。

A. 172.16.11.13　　B. 113.108.208.1　　C. 219.245.67.5　　D. 58.63.236.45

2. netstat-r 命令的功能是________。

A. 显示路由记录　　　　B. 查看连通性

C. 追踪 DNS 服务器　　D. 捕获网络配置信息

3. 在 Windows 命令行窗口中进入 Nslookup 交互工作方式，然后输入 set type=mx，这样的设置可以________。

A. 切换到指定的域名服务器　　B. 查询邮件服务器的地址

C. 由地址查找对应的域名　　　D. 查询域名对应的各种资源

11.7.4 同步练习参考答案

1. C　　　2. A　　　3. B

11.8 网络监视和管理工具

11.8.1 考点辅导

11.8.1.1 网络监听原理

在以太网中是基于广播方式传送数据的，也就是说，所有的物理信号都要经过其中的机器。如果将网卡置于混杂模式，那么网卡就能够接收到一切通过它的数据，而不管实际

上数据的目的地址是不是它。

对于网卡来说，一般有 4 种接收模式。

(1) 广播模式。在这种模式下，网卡能够接收网络中的广播信息。

(2) 组播模式。在这种模式下，网卡能够接收组播数据。

(3) 直接模式。在这种模式下，只有目的网卡才能接收该数据。

(4) 混杂模式。在这种模式下，网卡能够接收一切通过它的数据，而不管该数据是否是传给它的。

11.8.1.2 网络嗅探器

网络嗅探器(Sniffer)，顾名思义就是侦听器、嗅探器或窃听器。其工作原理是：将网卡工作模式设置成混杂模式(Promiscuous Mode)，把所有发送到该网卡的数据全部接收下来，再对接收下来的数据进行分析。Sniffer 可以是软件，也可以是硬件。硬件的 Sniffer 常常被称为网络分析仪。最常见的 Sniffer 的软件产品有 Sniffer PRO/NetXray，它是一款专业的协议分析工具。

将 Sniffer 放置于被攻击机器或网络附近，可以很轻松地截获在网上传送的用户姓名、口令、信用卡号码、截止日期、账号和 PIN(个人识别码)。比如偷窥机密或敏感的信息数据，通过拦截数据包，入侵者可以很方便地记录别人之间敏感的信息传送，或者干脆拦截整个 E-mail 会话过程。

11.8.1.3 Sniffer 软件的功能和使用方法

Sniffer 可以捕获用户的口令；可以截获机密的或专有的信息；也可以被用来攻击相邻的网络或者用来获取更高级别的访问权限。

1. Sniffer 的工作原理

通常在同一个网段的所有网络接口都有访问在物理媒体上传输的所有数据的能力，而每个网络接口都还应该有一个硬件地址，该硬件地址不同于网络中存在的其他网络接口的硬件地址，同时，每个网络至少还要有一个广播地址。在正常情况下，一个合法的网络接口应该只响应这样的两种数据帧：

- 帧的目标区域具有和本地网络接口相匹配的硬件地址。
- 帧的目标区域具有“广播地址”。

在接收到上面两种情况的数据包时，网卡通过 CPU 产生一个硬件中断，该中断能引起操作系统注意，然后将帧中所包含的数据传送给系统进一步处理。

Sniffer 就是一种能将本地网卡的状态设置成混杂模式的软件，当网卡处于混杂模式时，该网卡具备“广播地址”，它对所有遇到的每一个帧都产生一个硬件中断，以提醒操作系统处理流经该物理媒体的每一个报文包。

可见，Sniffer 工作在网络环境中的底层，它会拦截所有的正在网络上传送的数据，并且通过相应的软件处理，可以实时分析这些数据的内容，进而分析所处的网络状态和整体布局。

2. Sniffer 的工作环境

Sniffer 就是能够捕获网络报文的设备。嗅探器在功能和设计方面有很多不同，有些只

能分析一种协议，而另一些能够分析几百种协议。一般情况下，大多数的嗅探器至少能够分析下面的协议：标准以太网、TCP/IP、IPX、DECNet。

11.8.1.4　HP OpenView

常见的网络管理软件有 HP 公司的 OpenView、IBM 公司的 NetView、SUN 公司的 SUN Net Manager、Cisco 公司的 Cisco Works、3Com 公司的 Transcend 等。

HP 公司的 OpenView 是功能强大的网络和系统管理工具，是第一个跨平台的网络管理系统。OpenView 的应用和系统管理解决方案是由一些套件解决方案组成的。

(1) hp OpenView Operations：一体化网络和系统管理平台。

(2) hp OpenView Reporter：功能强大的管理报告解决方案。

(3) hp OpenView Performance：端到端资源和性能管理解决方案。

(4) hp OpenView GlancePlus：具有实时诊断和监控功能。

(5) hp OpenView GlancePlus Pak 2000：提供可全面管理系统可用性与性能的综合性产品。

(6) hp OpenView Database Pak 2000：对 hp 9000 服务器与数据库的性能和可用性进行管理。

这些模块相互依存、相互支持，成为功能强大的系统和应用管理平台，提供全面的集成化应用和系统管理功能。

hp OpenView Operations 是一种集成化网络与系统管理解决方案，它把网络管理与系统管理集成在一个统一的用户界面，共享消息数据库、对象数据库、拓扑数据库等中的数据。目前它有两个主要的版本，分别是 hp OpenView Operations for Windows 和 hp OpenView Operations for UNIX。hp OpenView Operations for Windows 管理服务器能支持数百个受控节点和数千个事件。它不仅可以通过服务视图来扩展传统的网络运营管理，还可以从任意地点进行跨平台的管理，这样用户可以从服务角度进行管理并获得在基本运行管理基础上创新的能力。hp OpenView Operations for UNIX 是由业务驱动的管理解决方案，作为分布式大型管理解决方案，它能监视、控制和报告网络环境的状态，实现超大型混合管理。

hp OpenView Performance 提供了一种对分布式网络的任一处资源和不同类型的系统性能进行端到端管理的解决方案。它收集数据，并把这些数据进行整理后转化为对用户有用的信息，最终以经济、有效的方式为用户提供最佳的服务级别；它还提供保持系统平滑运行的信息，使用户可以有效地控制和利用资源，及时调整多个分布式的系统环境，对系统中影响服务层和用户层的故障做出响应；同时还使系统管理员能有效扩展其管理范围，对远程和本地的系统进行有效管理和监控，从而在性能管理和问题分析、资源规划和服务管理等主要领域满足网络的分布式管理要求。hp OpenView Performance 目前有两个主要的版本，分别是 hp OpenView Performance Manager for UNIX 和 hp OpenView Performance Manager for Windows。

hp OpenView Database Pak 2000 对服务器与数据库的性能和可用性进行管理。它提供强大的系统性能与诊断功能；有效收集并记录系统与数据库统计数据及进行告警；能够检测关键事件并采取修复措施；提供 200 多种测量数据和 300 多种日志文件状态。利用安装在服务器上的 Database Pak 2000，可以及时地发现数据库与系统资源的性能问题，以防止进一步恶化，及时、有效地对系统和数据库进行管理。

hp OpenView Reporter 是为用户分布式的网络环境提供的廉价、灵活、易用的管理报告解决方案。它提供了标准和可定制报告，自动将 hp OpenView 在所有支持平台上获取的数据转化为网络可利用的重要管理信息。Reporter 使报告能经由 Web 浏览器发布，网络中能访问 Web 浏览器的每个人都可立即获得报告。

hp OpenView GlancePlus Pak 2000 是可全面管理系统性能的综合性产品。它不但具有 GlancePlus Pak 系列产品的所有功能，还增加了单一系统事件与可用性管理。其组件包括：功能强大的系统性能监控与诊断工具 GlancePlus；用于记录系统性能并针对即将发生的性能问题发送警报的 PerformanceAgent；允许网络检测影响系统性能与可用性的关键事件，并在这种事件发生时及时获得通知的 Single-System Event 和 Availability Management。这样，GlancePlus Pak 2000 不仅具有 Glance Plus 的实时诊断与监控功能以及 Performance Agent 软件的历史数据收集功能，还可监控网络系统中可能会影响性能的关键事件。

11.8.1.5 IBM Tivoili NetView

Tivoili NetView 是 IBM 公司的网络管理工具，能够提供整个网络的完整视图，实现对网络产品的管理。它采用 SNMP 对网络上的设备进行实时的监控，对网络中发生的故障进行报警，从而减少了系统管理的难度和管理工作量。

IBM Tivoili NetView 网络管理解决方案可以实现的功能主要包括以下几个。

(1) 网络拓扑管理。NetView 能够自动发现联网的 IP 节点，包括路由器、交换机、服务器和 PC 等，并自动生成拓扑结构。

(2) 网络故障管理。网络故障管理是网络管理的核心。NetView 的图形化网络拓扑结构可以迅速发现出现故障的资源，并帮助管理员分析故障原因。

(3) 网络性能管理。NetView 的 SnmpCollect 功能可以自动采集重要的网络性能数据，如 IP 流量、带宽利用率、出错包数量、丢弃包数量和 SNMP 流量等。

(4) 网络设备管理。Tivoili NetView 是使用最广泛的网络管理平台之一，支持业界标准 API，能够与主要网络设备厂商的设备管理软件方便地集成。

(5) 管理权限分配。NetView 可以为管理员定义不同的管理角色，不同的管理角色可以被授权管理不同地域范围的设备，没有权限管理的设备不会出现在网络拓扑视图中。

(6) Web 管理功能。NetView 通过 Web 控制台实现了分布式的网络管理。NetView Web 控制台为用户提供了一个灵活、可配置的环境，便于用户远程访问网络设备、浏览交换机的端口、检查路由器的工作状态、查看 MAC 地址等。

(7) 支持 MPLS 管理功能。NetView 7.1 支持对多协议标记交换设备的识别，并能对有关 MPLS 的数据进行查询，可以管理 LSR 设备。

(8) 交换机的故障定位。IBM Tivoili Switch Analyzer 提供了第二层交换设备的发现功能，能够识别包括第二层和第三层交换设备在内的各种设备之间的关系。正确地关联分析可以区分不同的设备，无论是 IP 寻址的端口，还是第二层交换机上非 IP 寻址的端口、板卡或插件。

11.8.1.6 Cisco Works for Windows

Cisco Works for Windows 是基于 Web 的网络管理解决方案，主要应用于中、小型企业网络，提供了一套功能强大、价格低廉且易于使用的监控和配置工具，用于管理 Cisco 的交

换机、路由器、集线器、防火墙和访问服务器等设备。使用 Ipswitch 公司的 WhatsUp Gold 工具，还可以管理网络打印机、工作站、服务器和其他网络设备。CiscoWorks for Windows 中包含下列组件。

(1) CiscoView。CiscoView 可以提供设备前后面板的视图，能够以不同颜色动态地显示设备状态，并提示对特定设备组件的诊断和配置功能。CiscoView 启动后可以从设备列表中选择要监视的设备。

(2) WhatsUp Gold。WhatsUp Gold 是一种基于 SNMP 的图形化网络管理工具，可以通过自动或手工创建网络拓扑结构图管理整个企业网络，支持监视多个设备，具有网络搜索、拓扑发现、性能检测和警报追踪等功能。

(3) 阈值管理。阈值管理器(Threshold Manager)能够在支持 RMON 的 Cisco 设备上设置阈值并提取事件信息，以增强排除网络故障的能力。

(4) Show Commands。Show Commands 使得用户不必记住各个设备的命令行语法，使用 Web 浏览器进行简单操作就可以获取设备的系统信息和协议信息。

11.8.2　典型例题分析

例 11-25　网络管理系统由网络管理站、网管代理、网络管理协议和管理信息库 4 个要素组成。当网管代理向管理站发送异步事件报告时，使用的操作是________。(2013 年上半年真题)

A. get　　B. get-next　　C. trap　　D. set

解析：本题考查网络管理中 SNMP 协议支持的服务原语。

Get 检索数据，Set 改变数据，GetNext 提供扫描 MIB 树和连续检索数据的方法，Trap 则提供从代理进程到管理站的异步报告机制。

答案：C

例 11-26　在 Windows 系统中监听发送给 NT 主机的陷入报文的程序是________。(2012 年下半年真题)

A. snmp.exe　　B. mspaint.com　　C. notepad.exe　　D. snmptrap.exe

解析：本题考查 Windows SNMP 服务的基本概念。

Windows NT 的 SNMP 的服务包括两个应用程序。一个是 SNMP 代理服务程序 snmp.exe，另一个是 SNMP 陷入服务程序 snmptrap.exe。snmp.exe 接收 SNMP 请求报文，根据要求发送响应报文，能对 SNMP 报文进行语法分析，ASN.1 和 BER 编码/译码，也能发送陷入报文，并处理 WinSockAPl 的接口。snmptrap.exe 监听发送给 NT 主机的陷入报文，然后把其中的数据传送给 SNMP，管理 API。

答案：D

11.8.3　同步练习

1. 某局域网访问 Internet 速度很慢，经检测发现局域网内有大量的广播包，采用

________方法不可能有效地解决该网络问题。

A. 在局域网内查杀 ARP 病毒和蠕虫病毒

B. 检查局域网内交换机端口和主机网卡是否有故障

C. 检查局域网内是否有环路出现

D. 提高出口带宽速度

2. 下面几个网络管理工具的描述中，错误的是______。

A. netstat 可用于显示 IP、TCP、UDP、ICMP 等协议的统计数据

B. sniffer 能够使网络接口处于混杂模式，从而可截获网络上传输的分组

C. winipcfig 采用 MS-DOS 工作方式显示网络适配器和主机的有关信息

D. tracert 可以发现数据包到达目标主机所经过的路由器和到达时间

11.8.4 同步练习参考答案

1. D　　2. C

11.9 网络存储技术

11.9.1 考点辅导

1. 廉价磁盘冗余阵列

廉价磁盘冗余阵列(Redundant Array of Inexpensive Disk，RAID)是利用一台磁盘阵列控制器管理一组磁盘驱动器，组成一个可靠的、快速的大容量磁盘系统。RAID 规范包括 RAID 0～RAID 7 等多个等级，目前投入到商业应用的有以下几种。

1) RAID 0

RAID 0 需要两个以上的磁盘驱动器，每个磁盘划分为不同的区块，数据按区块 A1、A2、A3…的顺序存储，数据访问采用交叉存取、并行传输的方式。这种系统具有最高的磁盘空间利用率，易管理，但系统的故障率高，属于非冗余系统。

2) RAID 1

由磁盘对组成，每一个工作盘都有其对应的镜像盘，上面保存着与工作盘完全相同的数据副本，具有最高的安全性，但磁盘空间利用率只有 50%。

3) RAID 2

采用了海明码纠错技术，用户需增加校验盘来提供单纠错和双纠错功能。对数据的访问涉及阵列中的每一个盘。大量数据传输时 I/O 性能较高，但不利于小批量数据传输，实际应用中很少使用。

4) RAID 3

把奇偶校验码存入一个独立的校验盘上。如果一个盘失效，其上的数据可以通过对其他盘上的数据进行异或运算得到。读数据很快，但因为写入数据时要计算校验位，速度较

慢。RAID3 主要用于图形图像处理等要求吞吐率比较高的场合，对于大量的连续数据可提供良好的传输速率，但对于随机数据，奇偶校验盘会成为写操作的瓶颈。

5)　RAID 5

各块独立硬盘进行条带化分割，相同的条带区进行奇偶校验(异或运算)，校验数据平均分布在每块硬盘上。以 n 块硬盘构建的 RAID 5 阵列可以有 $n-1$ 块硬盘的容量，磁盘空间利用率为 $(n-1)/n$。它是目前使用比较多的一种阵列。

6)　RAID 0+1

RAID 0+1 是 RAID 0 和 RAID 1 的组合形式，也称为 RAID 10。RAID 0+1 是存储性能和数据安全兼顾的方案。它提供与 RAID 1 同样的数据安全保障的同时，也提供了与 RAID 0 近似的访问速率。

7)　JBOD 模式

JBOD(Just a Bunch Of Drives)是在逻辑上将几个物理磁盘连接起来，组成一个大的逻辑磁盘。JBOD 不提供容错，其容量等于所有磁盘容量的总和。严格意义上说，JBOD 不属于 RAID 的范围。

2. *网络存储*

基于 Windows、Linux 和 UNIX 等操作系统的服务器称为开放系统，开放系统的数据存储方式如图 11-12 所示。

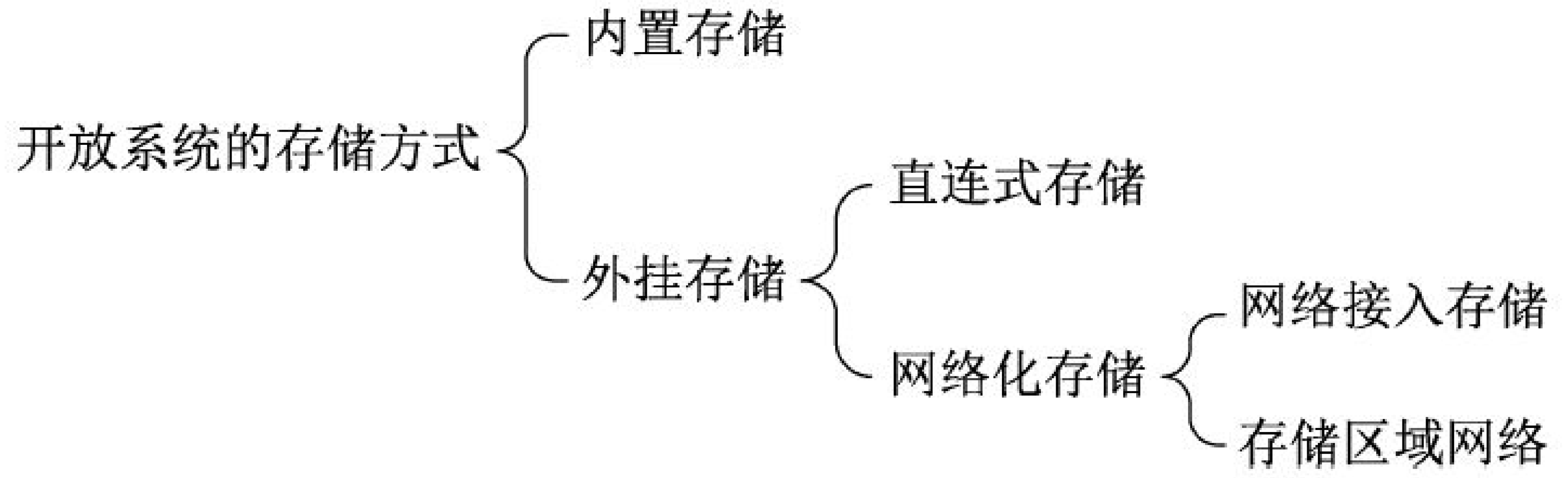


图 11-12　开放系统的数据存储方式

1)　直连式存储

直连式存储(Direct-Attached Storage，DAS)是在服务器外挂一组大容量磁盘，存储设备与服务器主机之间采用 SCSI 通道连接，带宽为 10Mb/s、20Mb/s、40Mb/s 和 80Mb/s 等。这种方式难以扩展存储容量，而且不支持数据容错功能，当服务器出现异常时，会造成数据丢失。

2)　网络接入存储

网络接入存储(Network Attached Storage，NAS)是将存储设备连接到现有的网络上，来提供数据存储和文件访问服务的设备。NAS 服务器是在专用主机上安装简化了的瘦操作系统的文件服务器。NAS 服务器内置了与网络连接所需要的协议，可以直接联网，具有权限的用户可以通过网络来访问 NAS 服务器中的文件。

3)　存储区域网络

存储区域网络(Storage Area Network，SAN)是一种连接存储设备和存储管理子系统的专用网络，专门提供数据存储和管理功能。SAN 是一种特殊的高速网络，采用光纤通道实现互联，通过光纤通道交换机连接存储阵列和文件服务器主机。SAN 不仅能提供大容量的存储数据，而且地域上可以分散部署，缓解了大量数据传输对局域网通信的影响。

11.9.2 典型例题分析

例 11-27 假如有 3 块容量是 300GB 的硬盘做 RAID 5 阵列，则这个 RAID 5 的容量是 __(63)__。(2017 年下半年真题 63)

A. 300GB B. 4500GB C. 600GB D. 900GB

解析：RAID 5 的容量占比为$(n-1)/n$，n 代表磁盘数量。

答案：C

11.9.3 同步练习

1. 下列说法错误的是________。

   A. RAID 0+1 是 RAID 0 和 RAID 1 的组合形式，也称为 RAID 01

   B. RAID 0 需要两个以上的磁盘驱动器，每个磁盘划分为不同的区块

   C. RAID 2 采用了海明码纠错技术，用户需增加校验盘来提供单纠错和双纠错功能

   D. RAID 3 把奇偶校验码存入在一个独立的校验盘上

2. 廉价磁盘冗余阵列(RAID)利用冗余技术实现高可靠性，其中 RAID 1 的磁盘利用率为 __(1)__。如果利用 4 个盘组成 RAID 3 阵列，则磁盘利用率为 __(2)__。

   (1)、(2) A. 25% B. 50% C. 75% D. 100%

3. 以下关于网络存储的描述正确的是______。

   A. SAN 系统是将存储设备连接到现有的网络上，其扩展能力有限

   B. SAN 系统是将存储设备连接到现有的网络上，其扩展能力很强

   C. SAN 系统使用专用网络，其扩展能力有限

   D. SAN 系统使用专用网络，其扩展能力很强

11.9.4 同步练习参考答案

1. A 2. (1) B (2) C 3. D

11.10 本 章 小 结

本章知识点在 2014 年的新大纲中改动不大，主要是知识点的明确化、具体化。

本章要求考生掌握网络管理的相关知识，包括网络管理的功能域、网络管理协议、网络管理命令、网络管理工具、网络管理平台和分布式网络管理。

本章相关知识点在历次考试中分布相对集中，分值在 8 分左右，是考试的重点。根据往年的考题，本章每节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

11.11　达标训练题及参考答案

11.11.1　达标训练题

1. 网络管理的五大功能域是________。

   A. 配置管理、故障管理、计费管理、性能管理和安全管理

   B. 配置管理、故障管理、计费管理、带宽管理和安全管理

   C. 配置管理、故障管理、成本管理、性能管理和安全管理

   D. 配置管理、用户管理、计费管理、性能管理和安全管理

2. 在 SNMP 中，当代理收到一个 GET 请求时，如果有一个值不可或不能提供，则返回________。

   A. 该实例的下个值　B. 该实例的上个值　C. 空值　D. 错误信息

3. SNMP 网络管理中，一个代理可以由________管理站管理。

   A. 0 个　B. 1 个　C. 2 个　D. 多个

4. Windows Server 2003 中配置 SNMP 服务时，必须以________身份登录才能完成 SNMP 服务的配置功能。

   A. Guest　B. 普通用户

   C. Administrators 组成员　D. Users 组成员

5. SNMPv2 提供了 3 种访问管理信息的方法，这 3 种方法不包括________。

   A. 管理站向代理发出通信请求　B. 代理向管理站发出通信请求

   C. 管理站与管理站之间的通信　D. 代理向管理站发送陷入报文

6. 下面有关 RMON 的论述中，错误的是________。

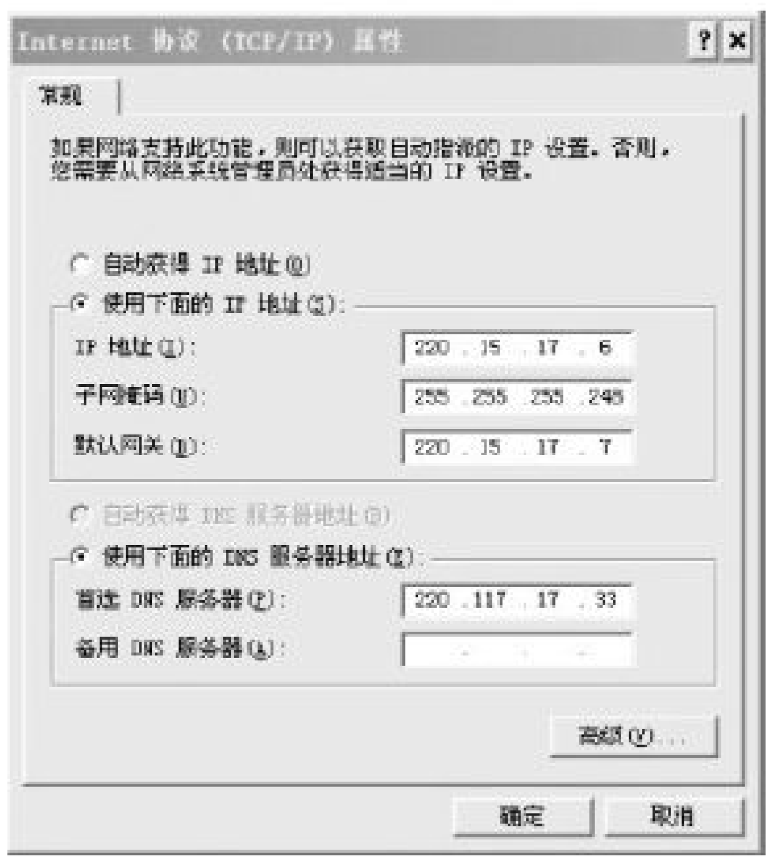
   A. RMON 的管理信息库提供整个子网的管理信息

   B. RMON 的管理信息库属于 MIB-Ⅱ的一部分

   C. RMON 监视器可以对每个分组进行统计和分析

   D. RMON 监视器不包含 MIB-Ⅱ的功能

7. 一台电脑的本地连接设置如下图所示，结果发现不能 ping 通任何网络设备，该故障的原因是________。



   A. 默认网关的地址不属于主机所在的子网

   B. 该主机的地址是一个广播地址

C. 默认网关的地址是该子网中的广播地址

D. 该主机的地址是一个无效的组播地址

8. 两个主机通过电缆直接相连，主机 A 的 IP 地址为 220.17.33.24/28，主机 B 的 IP 地址为 220.17.33.100/28，两个主机互相 ping 不通，这时应该________。

A. 改变主机 A 的地址为 220.17.33.15

B. 改变主机 B 的地址为 220.17.33.111

C. 改变子网掩码为/26

D. 改变子网掩码为/25

9. 在 Windows 命令行下执行______命令出现下图的效果。

```
Tracing route to Microsoft [157.54.1.196] over a maximum of 30h
0  172.16.67.35
1  172.16.67.216
2  192.166.52.1
3  192.166.80.1
4  157.54.247.14
5  157.54.1.196
Computing  statistics for 125 seconds…Source to Here This Node/Link
Hop    RTT    Lost/Sent =Pet   Lost/Sent=Pet    Address
0                                           172.16.87.35
                         0/100=0%         |
1      41ms   0/100=0%     0/100=0%      172.16.87.218
                         13/100=13%       |
2      22ms   16/100=16%     3/100=3%     192.168.52.1
                          0/100=0%        |
3      24ms   13/100=13%     0/100=0%     192.168.60.1
                          0/100=0%        |
4      21ms   14/100=14%     1/100=1%     157.54.247.14
                          0/100=0%       |
5      24ms   13/100=13%     0/100=0%      157.54.1.196
Trace complete.
```

A. pathping-n microsoft　　B. tracet-d microsoft

C. nslookup microsoft　　D. arp-a

10. 与 route print 具有相同功能的命令是______。

A. ping　　B. arp-a　　C. netstat-r　　D. tracert-d

11. 嗅探器改变了网络接口的工作模式，使得网络接口______。

A. 只能够响应发送给本地的分组　　B. 只能够响应本网段的广播分组

C. 能够响应流经网络接口的所有分组　　D. 能够响应所有组播信息

12. 在检查网络故障时，要确定目标主机是否有故障，只需向同一网段中的其他主机发__(1)__命令，如果可达，则可以确定是目标主机发生了故障；否则，故障就可能是由__(2)__引起的。如果问题是由路由配置不当引起的，则使用 traceroute 或 Windows 系统的__(3)__程序来跟踪一个数据报文__(4)__，以检测问题到底出在哪个环节上。如果 ping 成功，则问题很可能是出在__(5)__。

(1) A. ping　　B. traceroute　　C. trap　　D. get-request

(2) A. 本地配置错误　　B. 物理故障

C. 路由问题　　D. 以上都有可能

(3) A. traceroute　　B. traceroute-w　　C. route　　D. tracert

(4) A. 最大存在时间
B. 在经过不通网络或隧道时所加载的协议
C. 所到达远程主机的接口
D. 在主机间传送所经过的路径

(5) A. 网络系统配置方面　　B. 连接主机的物理线路断开
C. 核心　　D. 程序

13. Sniffer 是利用计算机的网络接口截获＿(1)＿的一种工具。Sniffer 可以将本地网卡状态设成“混杂”状态，当网卡处于这种“混杂”模式时，该网卡具备“广播地址”，它对遇到的每一个帧都产生一个＿(2)＿，以便提醒操作系统处理流经该物理媒体的每一个报文包。Sniffer 攻击主要有：＿(3)＿。Sniffer 通常运行在＿(4)＿上，或有路由器功能的主机上，这样就能对大量的数据进行监控。Sniffer 属＿(5)＿的攻击。通常是攻击者已经进入了目标系统，然后使用 Sniffer 这种攻击手段，以便得到更多的信息。

(1) A. 发给自己的数据报文　　B. 所有 ICMP 的数据报文
C. 目的地为其他计算机的数据报文　　D. 所有 UDP 的数据报文

(2) A. 软件中断　　B. 忽略报文　　C. 硬件中断　　D. 响应报文

(3) A. 捕获用户名和口令　　B. 获取更高级别的访问权限
C. 窥探低级的协议信息　　D. 以上都是

(4) A. 主机　　B. 路由器　　C. 服务器　　D. 防火墙

(5) A. 第一层次　　B. 第二层次　　C. 第三层次　　D. 所有层次

14. 在 IBM NetView 中，使用性能轮询与＿(1)＿来检测网络故障并响应。对第三方而言，NetView 在某种程度上提供了一些灵活性，在系统告警和事件中允许＿(2)＿。NetView 也使用了＿(3)＿，这使得利用 NetView 采集来的数据开发扩展应用变得相对容易。Sun Net Manager 提供一种＿(4)＿，这是一种介于集中式的网络管理和分散的、非共享的对象管理之间的网络管理方式。

(1) A. 状态轮询　　B. 业务轮询　　C. 流量分析　　D. 路由分析

(2) A. 忽视报警，维持最大限度网络运行　　B. 服务器自动处理网络故障
C. 调用用户自定义的程序　　D. 以上都错

(3) A. 分布式数据管理　　B. MIB 数据库
C. 文件备份和恢复系统　　D. 商业化的关系数据库

(4) A. 分布式网络管理　　B. 自动网络管理
C. 手工网络管理　　D. 集成的网络管理

11.11.2　参考答案

1. A　　2. A　　3. D　　4. C　　5. B　　6. D
7. C　　8. D　　9. A　　10. C　　11. C
12. (1) A　(2) D　(3) D　(4) D　(5) A
13. (1) C　(2) C　(3) D　(4) B　(5) B
14. (1) A　(2) C　(3) D　(4) D

第 12 章　网络规划和设计

大纲要求：

- 网络系统的需求分析，包括功能需求、性能需求、可靠性需求、安全需求、管理需求。
- 网络系统的设计，包括拓扑结构设计、信息点分布和通信量计算、结构化布线、链路冗余和可靠性、安全措施、网络设备的选型。
- 通信子网的设计，包括核心交换机的选型和配置、汇聚层的功能配置、接入层交换机的配置和部署。
- 资源子网的设计，包括网络服务和服务器的选型。
- 网络系统的构建和测试，包括安装工作、测试和评估、转换到新网络的工作计划。

12.1　结构化布线系统

12.1.1　考点辅导

结构化综合布线系统是基于现代计算机技术的通信物理平台，集成了语音、数据、图像和视频的传输功能，消除了原有通信线路在传输介质上的差别。

结构化综合布线系统包括以下内容。

- 建筑物综合布线系统(Premises Distribution System，PDS)。
- 智能大厦布线系统(Intelligent Building System，IBS)。
- 工业布线系统(Industry Distribution System，IDS)。

建筑物综合布线系统(PDS)是一个能够支持任何用户选择的话音、数据、图形、图像应用的电信布线系统。系统应能支持话音、图形、图像、数据多媒体、安全监控、传感等各种信息的传输，支持 UTP、光纤、STP、同轴电缆等各种传输载体，支持多用户、多类型产品的应用，支持高速网络的应用。

结构化综合布线系统应满足标准化、实用性、先进性、开放性、结构化和层次化的要求。

结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、管理子系统、干线子系统、设备间子系统和建筑群子系统，如图 12-1 所示。

1. 工作区子系统

工作区子系统是由终端设备到信息插座的整个区域，用于将用户终端设备连接到布线系统，主要包括信息插座、跳线、适配器。

信息插座的安装分为嵌入式安装和表面安装两种方式。信息插座通常安装在工作间四周的墙壁下方，距地面 30cm，也有的安装在用户办公桌上。通常一个信息插座需要 $90cm^2$ 的空间。

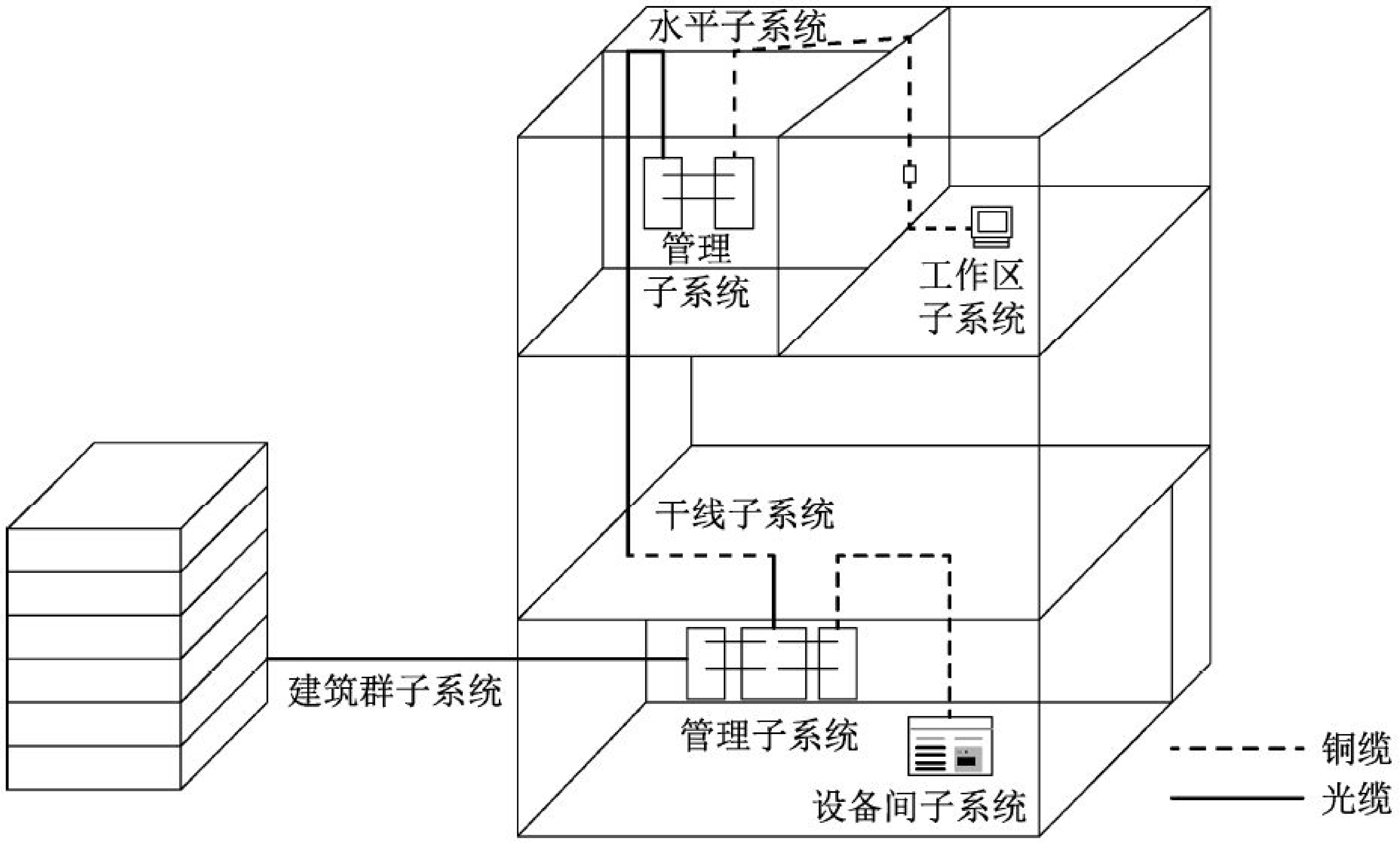


图 12-1　结构化布线系统的组成

2. 水平子系统

水平子系统是结构化综合布线系统中连接用户工作区与布线系统主干的子系统。水平子系统由每层配线间至信息插座的配线电缆和工作区用的信息插座等组成。在结构化综合布线系统中，水平布线子系统起着支线的作用，它将所有用户端通过一些连接件连接到配线设备上。

水平布线的布线通道有两种：一种是暗管预埋、墙面引线方式；另一种是地下管槽、地面引线的方式。

3. 管理子系统

管理子系统是结构化布线系统中对布线电缆进行端接及配线管理的子系统，通常设置在楼层的接线间内。

管理子系统由各种交连设备(双绞线跳线架、光纤跳线架)以及集线器和交换机等交换设备组成。交连设备通过水平布线子系统连接到各个工作区的信息插座，集线器或交换机与交连设备之间通过短线缆互连，这些短线称为跳线。

4. 干线子系统

干线子系统是结构化综合布线系统中连接各管理间、设备间的子系统，又称垂直子系统。综合布线系统的干线可根据距离的远近和用户对传输速率及传输质量的要求，选择多对数双绞线或光缆。一般在楼内的语音通信采用三类的大对数双绞线作为主干；数据通信可以采用高品质的五类双绞线，也可以采用光缆；如果电磁干扰严重，则推荐采用光缆作为数据主干。在做干线子系统的设计时，首先要确定每一层楼的干线需求，总结出整座楼的干线总体需求，确定干线电缆的种类及其大小尺寸，然后确定干线电缆的路由通道。

5. 设备间子系统

设备间子系统主要用来安放网络关键设备，地位十分重要。并非每一个综合布线系统

都有设备间子系统，但在大型建筑物中一般是有的，而且有时还不止一个。设备间子系统中的电话、数据、计算机主机设备及其保安配线设备宜设在一个房内。必要时，也可以分别设置，但程控交换机及计算机主机房距离设备间不宜太远。设备间的位置及大小应根据设备的数量、规模、最佳网络中心等内容综合考虑确定。在设备间子系统的设计和安装过程中还需要综合考虑配电系统(不间断电源)和安全因素(设备接地等)。

6. 建筑群子系统

建筑群子系统是结构化综合布线系统中由连接楼群之间的通信传输介质及各种支持设备组成的子系统。建筑群子系统也称为户外子系统，其传输介质除了各种有线手段外，还包含其他无线通信手段，如微波、无线电通信等。

户外电缆在进入大楼时通常在入口处经过一次转接接入户内系统，在转接处可以加上电器保护设备。现代化电话通信系统中通信线路在进入楼群时一般都考虑这一点，主要是避免因雷击或与高压线接触而给人和设备安全带来的损失。建筑群子系统布线方式有以下几种：地下管道敷设方式、直埋沟内敷设方式和架空等，不同方式各有其优、缺点。

在进行结构化布线系统设计时，要注意线缆长度的限制。表 12-1 给出了 EIA/TIA-568 标准提出的布线距离最大值。

表 12-1　布线距离

子 系 统	光纤/m	屏蔽双绞线/m	无屏蔽双绞线/m
建筑群(楼栋间)	2000	800	700
主干(设备间到配线间)	2000	800	700
配线间到工作区信息插座		90	90
信息插座到网卡		10	10

12.1.2　典型例题分析

例 12-1　结构化综合布线系统分为 6 个子系统，其中水平子系统的作用是__(67)__，干线子系统的作用是__(68)__。(2017 年上半年真题 67、68)

(67)、(68)　A. 实现各楼层设备间子系统之间的互联
　　B. 实现中央主配线架和各种不同设备之间的连接
　　C. 连接干线子系统和用户工作区
　　D. 连接各个建筑物中的通信系统

解析：水平子系统目的是实现信息插座和管理子系统(跳线架)之间的连接。干线子系统的作用是通过骨干线缆将主设备间和各楼层配线间体系连接起来。

答案：(67) C　(68) A

例 12-2　结构化布线系统分为 6 个子系统，其中干线子系统的作用是__(29)__。(2016 年下半年真题 29)

A. 连接各个建筑物中的通信系统
B. 连接干线子系统和用户工作区
C. 实现中央主配线架与各种不同设备之间的连接

D. 实现各楼层设备间子系统之间的互连

解析：干线子系统是结构化综合布线系统中连接各管理间、设备间的子系统，又称垂直子系统。

答案：D

12.1.3　同步练习

1. 结构化布线系统分为 6 个子系统，其中水平子系统的作用是 __(1)__ ，干线子系统的作用是 __(2)__ 。

(1)、(2) A. 连接各个建筑物中的通信系统
B. 连接干线子系统和用户工作区
C. 实现中央主配线架与各种不同设备之间的连接
D. 实现各楼层设备间子系统之间的互连

2. 结构化综合布线系统中的干线子系统是指________。

A. 管理楼层内各种设备的子系统　　B. 连接各个建筑物的子系统
C. 工作区信息插座之间的线缆子系统　　D. 实现楼层设备间连接的子系统

12.1.4　同步练习参考答案

1. (1) B　(2) A　　2. D

12.2　网络分析与设计过程

12.2.1　考点辅导

12.2.1.1　网络系统生命周期

一般来说，网络生命周期至少包括网络系统的构思和计划、分析和设计、运行和维护的过程。网络系统的生命周期是一个循环迭代的过程，每一个迭代周期都是网络重构的过程。常见的迭代周期构成方式主要有 3 种。

1. 四阶段周期

4 个阶段为构思与规划阶段、分析与设计阶段、实时与构建阶段、运行与维护阶段。其特点是能够快速适应新的需求变化，工作成本低，适用于网络规模较小、需求较为明确、网络结构简单的网络工程。

2. 五阶段周期

这是一种较为常见的迭代周期划分方法，它将一次迭代划分成 5 个阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。每个阶段都是一个工作环节，每个

环节完毕后才能进入到下一个环节，一般情况下不允许返回到前面的阶段。

3. 六阶段周期

六阶段周期是对五阶段周期的补充，分为需求分析、逻辑设计、物理设计、优化设计、实施及测试、检测及性能优化。

12.2.1.2 网络开发过程

根据五阶段迭代周期的模型，网络开发过程可以被划分为 5 个阶段。

1. 需求分析

需求分析是开发过程中最关键的阶段。不同的用户有不同的网络需求，收集的需求范围包括业务需求、用户需求、应用需求、计算机平台需求、网络通信需求，同时要考虑未来的需要，以便在以后对网络实现扩展。

需求分析的输出是产生一份需求说明，也就是需求规范。在写完需求说明书后，管理者和网络设计者应达成共识，并在文件上签字，这是规避网络建设风险的关键。

2. 现有网络系统的分析

如果网络开发过程是对现有网络的升级和改造，就必须进行现有网络系统的分析工作。现有网络系统分析的目的是描述资源分布，以便在升级时尽量保护已有的投资。

在这一阶段应给出一份正式的通信规范说明文档，作为下一阶段的输入。通信规范说明文档包括以下内容。

(1) 现有网络的拓扑结构。

(2) 现有网络的容量以及新网络所需的通信量和通信模式。

(3) 详细的统计数据，直接反映现有网络性能的测量值。

(4) Internet 接口和广域网提供的服务质量报告。

(5) 限制因素列表，如使用线缆和设备清单等。

3. 确定网络逻辑结构

网络逻辑结构设计阶段是体现网络设计核心思想的关键阶段，在这一阶段根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。网络逻辑结构大致描述了设备的互联及分布范围，但是不确定具体的物理位置和运行环境。

这个阶段应得到一份逻辑设计文档，输出内容包括以下几点。

(1) 网络逻辑设计图。

(2) IP 地址分配方案。

(3) 安全管理方案。

(4) 具体的软/硬件、广域网连接设备和基本的网络服务。

(5) 招聘和培训网络员工的具体说明。

(6) 对软硬件费用、服务提供费用以及员工和培训费用的初步估计。

4. 确定网络物理结构

物理网络设计是逻辑网络设计的具体实现，通过对设备的具体物理分布、运行环境等

的确定来确保网络的物理连接符合逻辑设计的要求。

这一阶段应得到一份网络物理结构设计文档，输出的内容包括以下几点。

(1) 网络物理结构图和布线方案。

(2) 设备和部件的详细列表清单。

(3) 软、硬件和安装费用的估算。

(4) 安装日程表，详细说明服务的时间及期限。

(5) 安装后的测试计划。

(6) 用户的培训计划。

5. 安装和维护

安装是根据前面的工程结果实施环境准备、设备安装调试的过程。安装阶段的主要输出就是网络本身。网络安装完成后，接收用户的反馈意见和监控网络的运行是网络管理员的任务。

12.2.1.3　网络设计的约束因素

一般来说，网络设计的约束因素主要来自政策、预算、时间和应用目标等方面。

(1) 政策约束的具体表现是法律法规条文，以及国际、国家和行业标准等。

(2) 预算是决定网络设计的关键因素。网络预算一般分为一次性投资预算和周期性投资预算。一般来说，年度发送的周期性投资预算和一次性投资预算之间的比例为 10%～15% 比较合理。

(3) 项目进度表限定了项目最后的限期和重要的阶段。通常，项目进度由客户负责管理。

(4) 通过应用目标检查，可以避免用户需求的缺失。检查形式包括设计小组内的自我检查和用户主管部门的确认检查两种。

12.2.2　典型例题分析

例 12-3　在网络规划和设计过程中，选择网络技术时要考虑多种因素。下面的各种考虑中不正确的是__(70)__。(2016 年下半年真题 70)

A. 网络带宽要保证用户能够快速访问网络资源

B. 要选择具有前瞻性的网络新技术

C. 选择网络技术时要考虑未来网络扩充的需求

D. 通过投入产出分析确定使用何种技术

解析：在进行正确的网络技术选择时，应该考虑通信带宽、技术成熟性、连接服务类型、可扩充性、高投资产出比等因素。有些新的应用技术在尚没有大规模投入应用时，还存在着较多不确定因素，而这些不确定因素将会给网络建设带来很多不可估量的损失。虽然新技术的自身发展离不开工程应用，但是对于大型网络工程来说，项目本身不能成为新技术的试验田。因此，尽量使用较为成熟、拥有较多案例的技术是明智的选择。

答案：B

12.2.3 同步练习

1. 搭建试验平台、进行网络仿真是网络生命周期中________阶段的任务。
   A. 需求规范　B. 逻辑网络设计　C. 物理网络设计　D. 实施
2. 网络系统设计过程中，物理网络设计阶段的任务是________。
   A. 依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境
   B. 分析现有网络和新网络的各类资源分布，掌握网络所处的状态
   C. 根据需求规范和通信规范，实施资源分配和网络规划
   D. 理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

12.2.4 同步练习参考答案

1. B　　2. A

12.3 网络需求分析

12.3.1 考点辅导

12.3.1.1 需求分析的范围

网络需求分析是网络开发过程的起始部分，这一阶段应明确客户所需的网络服务和网络性能。

在需求分析过程中，需要考虑以下几个方面的需求。

- 业务需求。
- 用户需求。
- 应用需求。
- 计算机平台需求。
- 网络需求。

1. 业务需求

网络系统是为一个集体提供服务的，对于该集体内的不同用户，需要收集特定的业务信息，包括以下内容。

(1) 确定结构组织。业务需求的第一步就是获取组织结构图，了解集体中的岗位设置及岗位职责。

(2) 确定关键时间点。对于大型项目，必须制订严格的项目实施计划，确定各个阶段关键的时间点。

(3) 确定网络投资规模。在整个网络的设计和实施中，费用是一个主要考虑的因素。

(4) 确定业务活动。主要通过对业务的分析，形成各类业务的网络需求，主要包括最

大用户数、并发用户数、峰值带宽和正常带宽等。

(5) 预测增长率。通过对网络发展趋势的分析，明确网络的伸缩性需求。

(6) 确定网络的可靠性和可用性。网络设计人员在进行需求分析的过程中，首先应获取行业的网络可靠性和可用性标准，并根据标准与用户进行交流，确定特殊的要求。

(7) 确定 Web 站点和 Internet 连接。

(8) 确定网络的安全性。

(9) 确定远程接入方式。

2. 用户需求

收集用户需求是要找出用户需要的重要服务和功能。收集用户需求的机制主要包括与用户群的交流、用户服务和需求归档 3 个方面。

收集用户需求最常用的方式有观察和问卷调查、集中访谈、采访关键人物。在整个设计和实施阶段，应始终保持与关键人员之间的交流，以确保网络工程建设不偏离用户需求。

用户服务表用于表示收集和归档的需求信息，也用来指导管理人员和网络用户进行讨论。

3. 应用需求

收集应用需求可以从两个角度出发：应用类型和应用对资源访问的角度。

(1) 按功能对应用进行分类，可以将应用划分为常见功能类型和特定功能类型。

(2) 按共享分类，可以将软件分为单用户软件、多用户软件和网络软件。

(3) 按响应方式分类，应用可以分为实时和非实时两种。

(4) 按网络规模分类，应用分为单机软件、对等网络软件、C/S 软件、BPS 软件和分布式软件等。

用户对网络资源的访问，是可以通过各种指标进行量化的，需要考虑的指标包括每个应用的用户数量、每个用户平均使用每个应用的频率、使用高峰期、平均访问时间长度、每个事务的平均大小、每次传输的平均通信量和影响通信的定向特性。

4. 计算机平台需求

需要调查的计算机平台主要分为个人计算机、工作站、小型机、中型机和大型机。

这一阶段的输出是计算机平台需求表，它是总结用户对计算机平台的需求的表格。

5. 网络需求

需求分析的最后工作是考虑网络管理员的需求，包括以下内容。

(1) 局域网功能。对于升级的网络，可以对现有网段划分方式进行改进，形成新的划分方案。对于新建的网络，要和网络管理员一起商量网段的划分方式。

(2) 网络性能。主要考虑的是网络容量和响应时间。

(3) 有效性需求。有效性条件没有固定的模式，通常要对局域网的拓扑结构、网络设备、服务器主机、存储设备、安全设备、机房设备和产品供应商等设定一些选择标准或过滤条件。

(4) 数据备份和容灾中心需求。根据不同的网络工程规模，存在两种建设情况，一种是需要建设复杂的数据中心和容灾备份中心，另一种是仅建立数据备份和容灾机制。

(5) 网络管理需求。网络管理建设要从网络管理目的、网络管理要素、要管理的网络资源、软件资源管理和软件分发、应用管理等几个方面进行调查。

(6) 网络安全需求。安全技术措施包括机房及物理线路安全、网络安全、系统安全、应用安全、安全信任体系等。

(7) 城域网/广域网的选择。可供选择的连接方案有两种，即点对点线路交换服务和分组交换服务。

12.3.1.2 编制需求说明书

编写需求说明书的目的是能够向管理人员提供决策用的信息，因此需求说明书应该做到尽量简明且信息充分。

对网络需求说明书存在两点要求。首先，无论需求说明书的组织形式如何，都应包含业务、用户、应用、计算机平台和网络 5 个方面的需求内容。其次，为了规范需求说明书的编制，一般情况下，需求说明书应该包括以下 5 个部分。

(1) 综述。

(2) 需求分析阶段总结。

(3) 需求数据总结。

(4) 按优先级排队的需求清单。

(5) 申请批准部分。

12.3.2 典型例题分析

例 12-4 在网络设计和实施过程中要采取多种安全措施，下面的选项中属于系统安全需求措施的是__(68)__。(2016 年下半年真题 68)

A. 设备防雷击　　B. 入侵检测

C. 漏洞发现与补丁管理　　D. 流量控制

解析：设备防雷击属于机房及物理线路安全需求；入侵检测、流量控制属于网络安全需求；漏洞发现与补丁管理属于系统安全需求。

答案：C

例 12-5 下列不属于需求说明书应该包括部分的是________。

A. 综述　　B. 需求分析阶段总结

C. 需求数据总结　　D. 应用

解析：需求说明书应该包括以下 5 个部分：综述、需求分析阶段总结、需求数据总结、按优先级排队的需求清单、申请批准部分。

答案：D

12.3.3 同步练习

网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行，

其中数据库容灾属于________。

A. 物理线路安全和网络安全　　　　B. 应用安全和网络安全

C. 系统安全和网络安全　　　　　　D. 系统安全和应用安全

12.3.4　同步练习参考答案

D

12.4　通信流量分析

12.4.1　考点辅导

1. 通信流量分析的方法

80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：通信流量的 80%是在某个网段中流动，只有 20%的通信流量访问其他网段。80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

但现在的网络，由于应用多样、资源分布分散等特性，使 80/20 规则出现翻转，即 80%的流量分配给远程，20%的流量在本地。这些需要应根据网络业务特性决定。

2. 通信流量分析的步骤

通信流量分析的步骤如下。

(1)　把网络分成易管理的网段。

网段划分要考虑用户的需求，一般情况是按工作组或部分来划分网段。由于网段属于局域网络范畴，在进行分析工作前，需要确定网段的局域网通信边界。如果网段的通信边界是物理边界，则这个网段需要独立进行分析；如果多个网段的通信边界是逻辑边界，则这些网段不需要独立进行分析，而作为一个整体网段来进行分析。

无论是物理网段分析，还是多个虚拟网段构成的整体网段分析，都可以采用局部分析法。局部分析法的实质在于只关注一个网段，并将网段边界外的其他部分等同于一个外部网络来进行分析。

(2)　确定个人用户和网段的通信量。

这个步骤的工作在于将需求分析中不同格式的统计表格转化为统一的流量表格，以便于开始后续的分析工作。

(3)　确定本地和远程网段上通信流量的分布。

这个步骤的重要任务是明确多少通信流量存在于网络内部，以及多少通信流量是访问其他网段。

(4)　对每个网段重复上述步骤。

(5)　分析广域网和网络骨干的通信流量。

通信流量计算完成后，要把它们整理总结成一份文件，该文件将成为最终的通信规范

说明书的一部分。

12.4.2 典型例题分析

例 12-6 在网络设计阶段进行通信流量分析时可以采用简单的 80/20 规则，下面关于这种规则的说明中，正确的是______。

A. 这种设计思路可以最大限度满足用户的远程联网需求

B. 这个规则可以随时控制网络的运行状态

C. 这个规则适用于内部交流较多而外部访问较少的网络

D. 这个规则适用的网络允许存在具有特殊应用的网段

解析：80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：通信流量的 80%是在某个网段中流动，只有 20%的通信流量访问其他网段。80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

答案：C

12.4.3 同步练习

假设网络的生产管理系统采用 B/S 工作方式，经常上网的用户数为 100 个，每个用户每分钟平均产生 11 个事务，平均事务量大小为 0.06MB，则这个系统需要的信息传输速率为________。

A. 5.25Mb/s　　B. 8.8Mb/s　　C. 66Mb/s　　D. 528Mb/s

12.4.4 同步练习参考答案

B

12.5 逻辑网络设计

12.5.1 考点辅导

12.5.1.1 逻辑网络设计的目标

一般情况下，逻辑网络设计的目标如下。

- 合适的应用运行环境。
- 成熟、稳定的技术选型。
- 合理的网络结构。
- 合适的运营成本。

- 逻辑网络的可扩充性能。
- 逻辑网络的易用性。
- 逻辑网络的可管理性。
- 逻辑网络的安全性。

12.5.1.2　需要关注的问题

逻辑网络设计需要关注以下问题。

(1) 设计要素。包括用户需求、设计限制、现有网络、设计目标。

(2) 设计面临的冲突。设计目标是一个复杂的整体，由不同维度的子目标构成。这些子目标之间可能存在冲突。

(3) 成本与性能。成本与性能是最为常见的冲突目标。一般来说，网络设计方案的性能越高，也就意味着更高的成本，包括建设成本和运行成本。

12.5.1.3　主要的网络服务

对于大多数网络来说，都存在着两个主要的网络服务——网络管理和网络安全。

1. 网络管理

网络管理的重点内容是网络故障诊断、网络配置以及重配置和网络监视。

2. 网络安全

网络安全系统是网络逻辑设计的固有部分，可以采用以下步骤进行安全设计。

(1) 明确需要安全保护的系统。

(2) 确定潜在的网络弱点和漏洞。

(3) 尽量简化、安全。

(4) 制定安全制度。

12.5.1.4　技术评价

在进行正确的网络技术选择时，应该考虑通信带宽、技术成熟性、连接服务类型、可扩充性、高投资产出比等因素。

12.5.1.5　逻辑网络设计的工作内容

逻辑网络设计的工作内容主要有网络结构的设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理、网络安全和逻辑网络设计文档，并根据这些设计选择设备和服务供应商。

12.5.2　典型例题分析

例 12-7　网络设计过程包括逻辑网络设计和物理网络设计两个阶段，各个阶段都要产生相应的文档。下面的选项中，属于逻辑网络设计文档的是__(69)__，属于物理网络设计文档的是__(70)__。(2016 年上半年真题 69、70)

(69)、(70)　A. 网络 IP 地址分配方案　　　B. 设备列表清单

C. 集中访谈的信息资料　　　　　　　　D. 网络内部的通信流量分布

解析：逻辑网络设计的任务是根据需求规范和通信规范，实施资源分配和安全规划。主要包括：层次网络结构设计；物理层技术选择；局域网技术选择与应用；广域网技术选择与应用；地址设计与命名模型；路由选择协议；网络管理；网络安全；逻辑网络设计文档。

物理网络设计的任务是设计特定的物理环境平台，主要包括结构化综合布线系统的设计、机房环境设计、传输介质及网络设备选型及安装方案、特殊设备安装方案和网络实施等。

答案：(69) A　(70) B

12.5.3　同步练习

网络系统设计过程中，逻辑网络设计阶段的任务是______。

A. 对现有网络资源进行分析，确定网络的逻辑结构

B. 根据需求说明书确定网络的安全系统架构

C. 根据需求规范和通信规范，分析各个网段的通信流量

D. 根据用户的需求，选择特定的网络技术、网络互连设备和拓扑结构

12.5.4　同步练习参考答案

D

12.6　网络结构设计

12.6.1　考点辅导

12.6.1.1　局域网的结构

1. 单核心局域网的结构

单核心局域网的结构主要由一台核心 2 层或 3 层交换设备构建局域网的核心，通过多台接入交换机接入计算机节点，该网络一般通过与核心交换机互联的路由设备接入广域网，如图 12-2 所示。

2. 双核心局域网的结构

双核心局域网的结构主要由两台核心交换设备构建局域网核心，该网络一般也是通过与核心交换机互联的路由设备接入广域网，并且路由器与两台核心交换设备之间都存在物理链路，如图 12-3 所示。

3. 环型局域网的结构

环型局域网的结构由多台核心 3 层设备连接成双 RPR 动态弹性分组环，构成整个局域网络的核心，该网络通过与环上交换设备互联的路由设备接入广域网络，如图 12-4 所示。

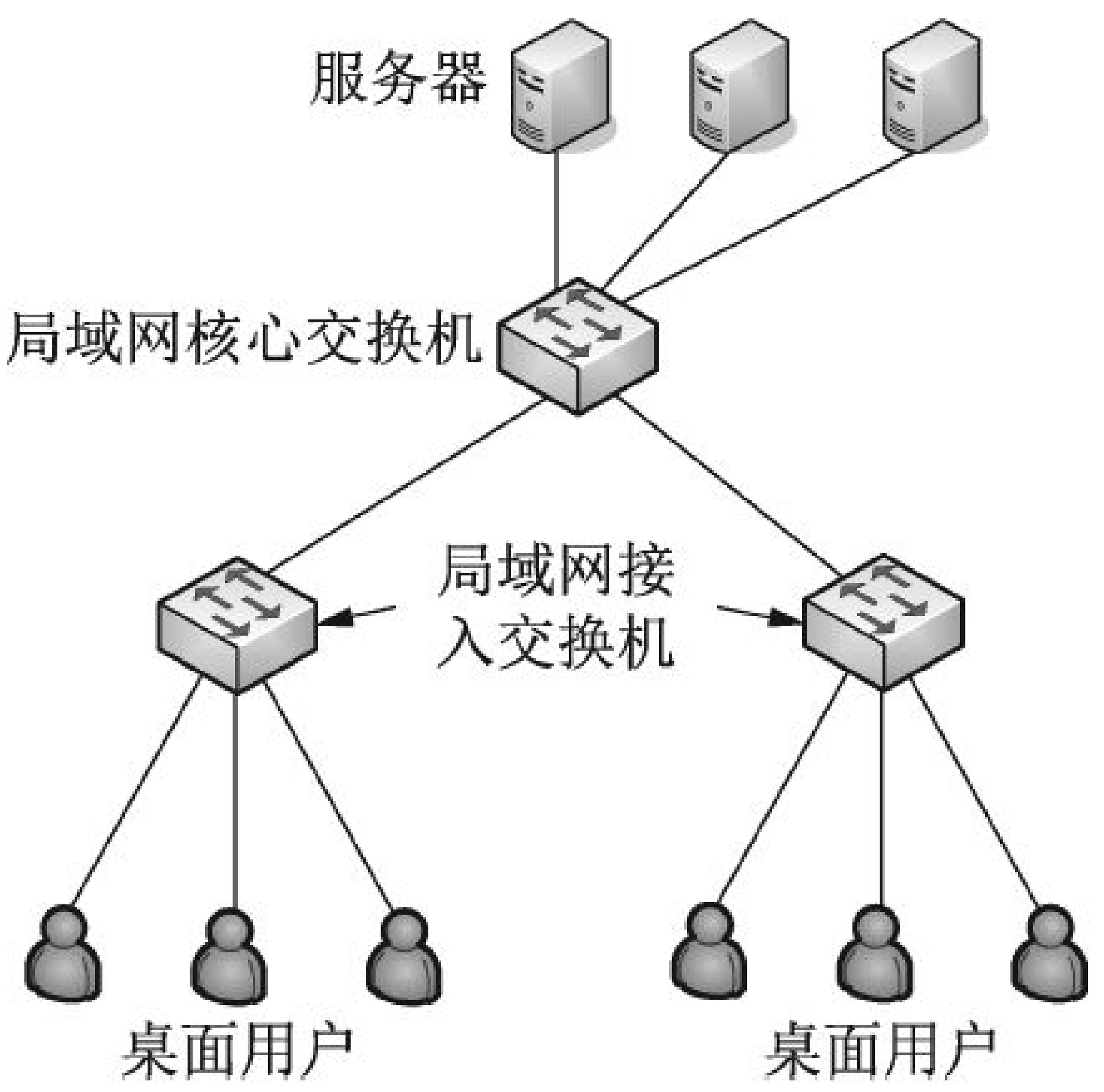


图 12-2　单核心局域网的结构

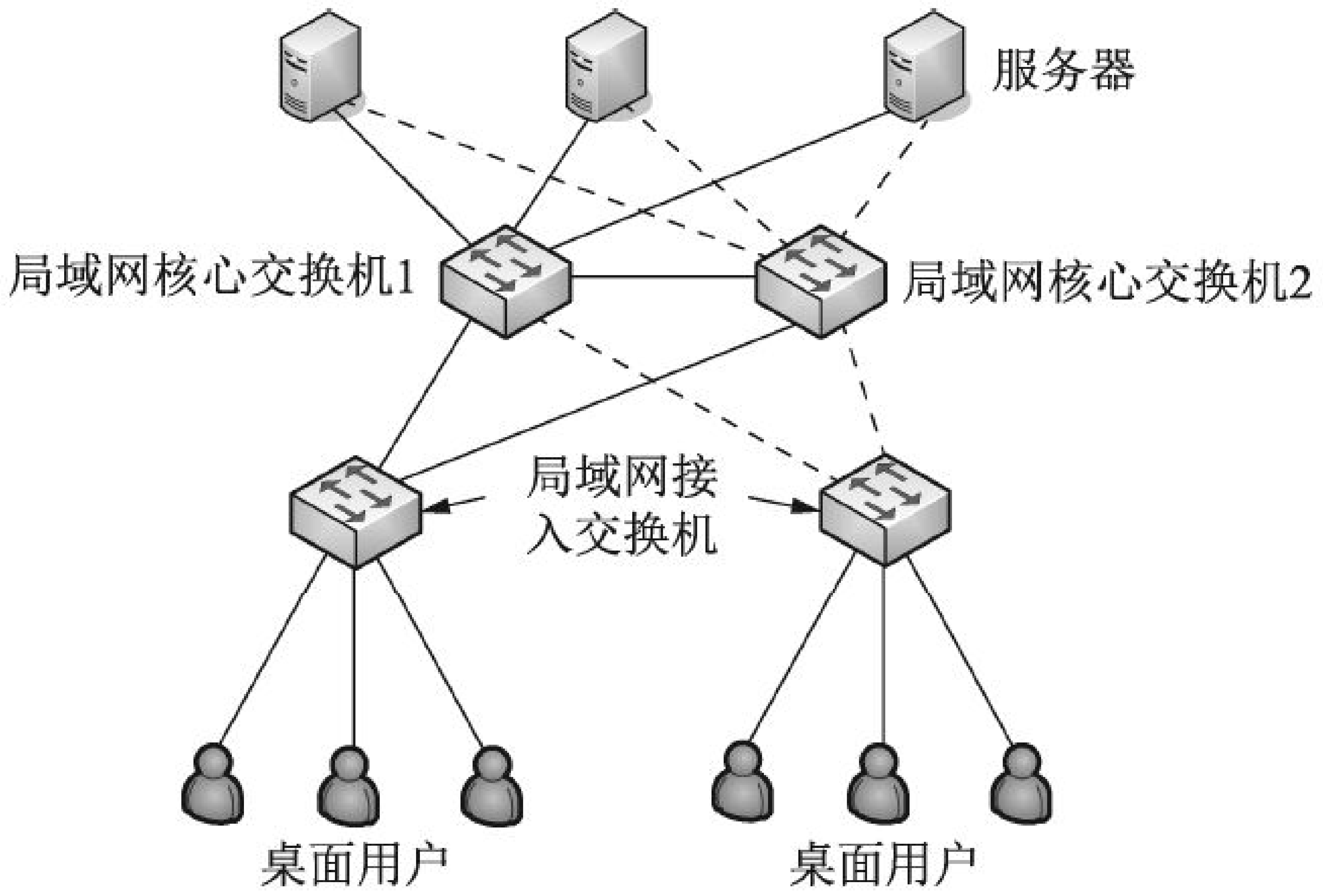


图 12-3　双核心局域网的结构

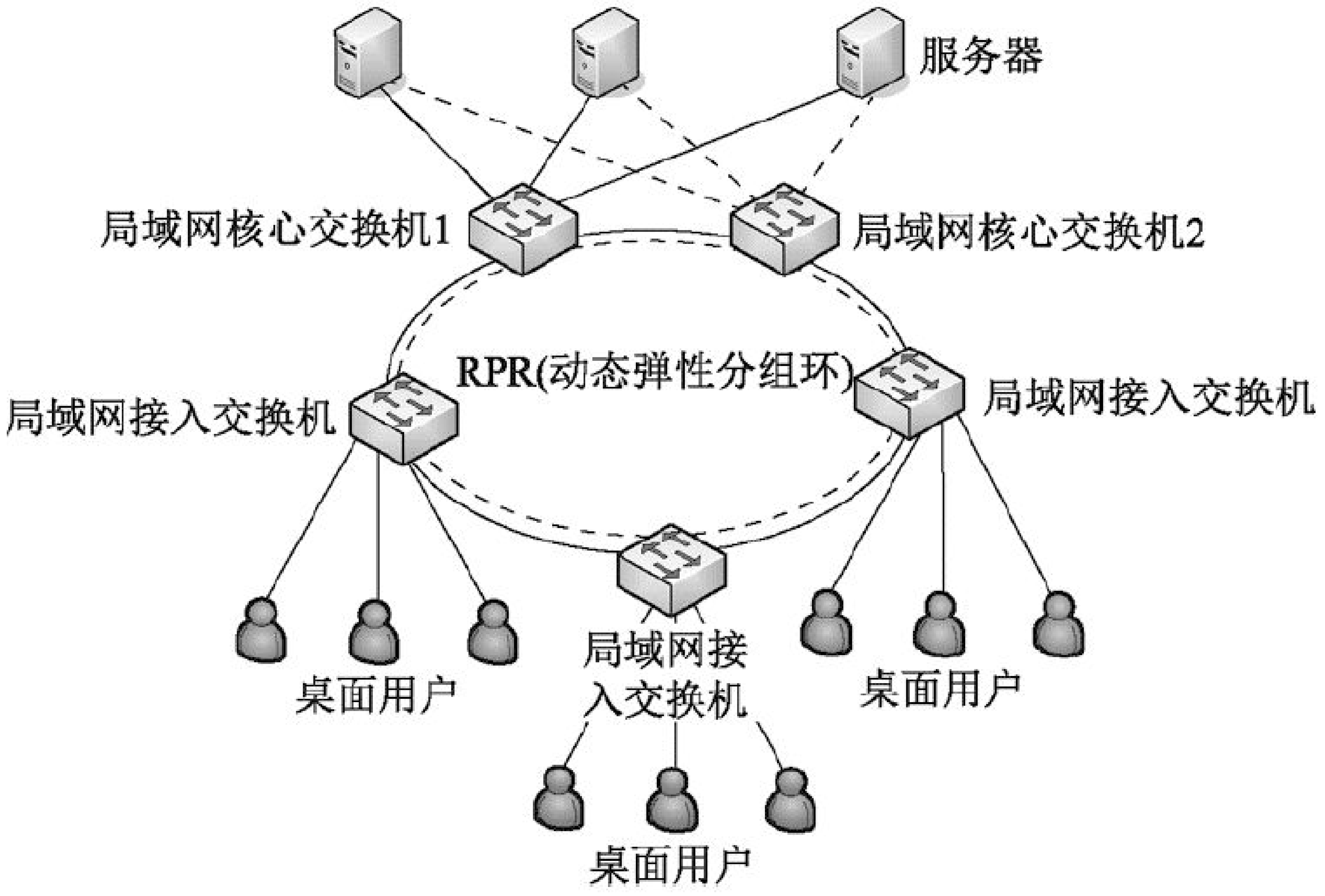


图 12-4　环型局域网结构

4. 层次局域网的结构

层次结构主要定义了根据功能要求不同将局域网络划分层次构建的方式，从功能上定义了核心层、汇聚层和接入层。层次局域网一般通过与核心层设备互联的路由设备接入广域网络，如图 12-5 所示。

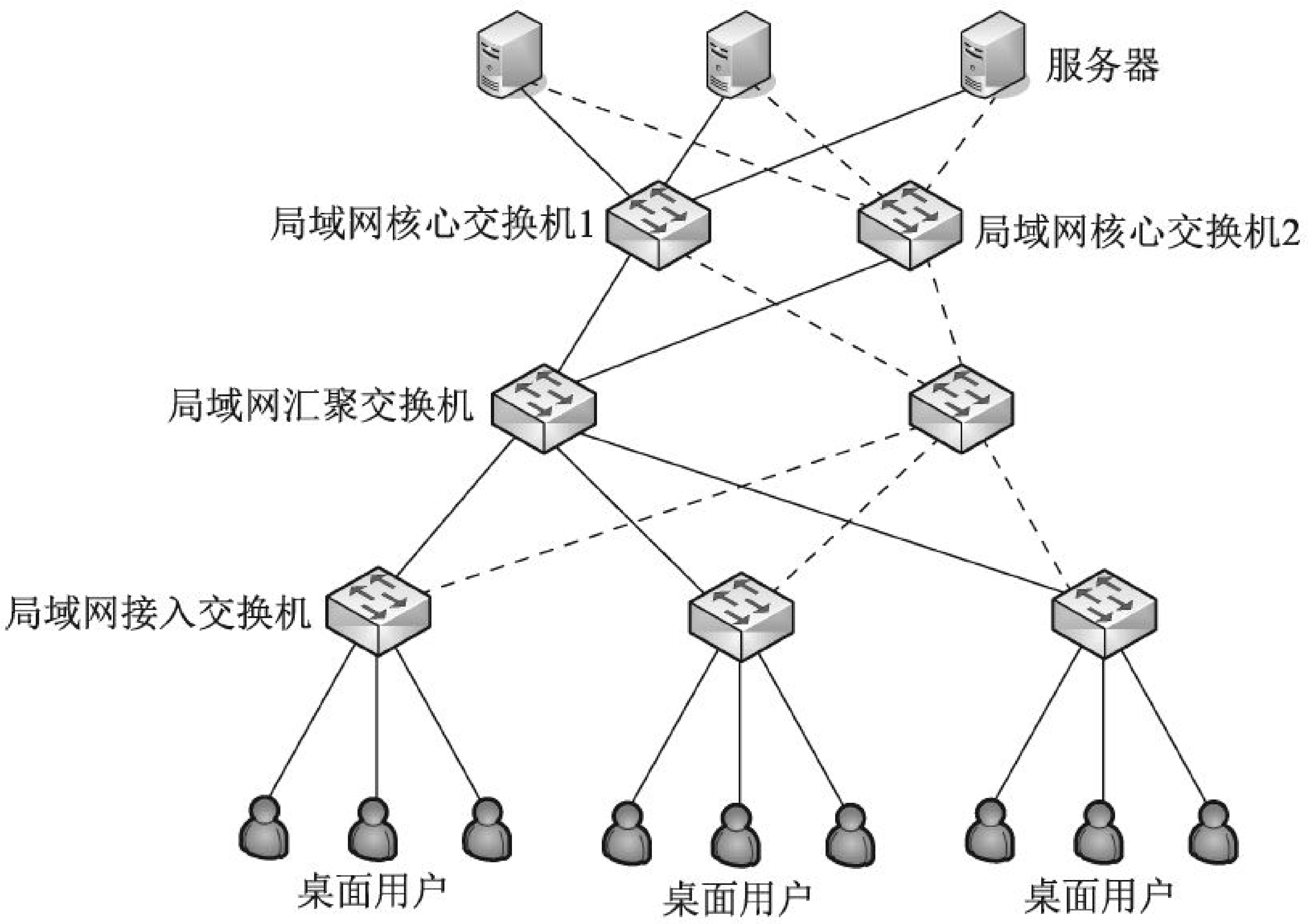


图 12-5　层次局域网的结构

12.6.1.2　层次化网络的设计

1. 层次化网络的设计模型

层次化网络设计模型已经成为网络主流的园区网络的经典模型。一个典型的层次化网络结构应具有以下特征。

(1) 由经过可用性和性能优化的高端路由器和交换机组成的核心层。

(2) 由用于实现策略的路由器和交换机构成的汇聚层。

(3) 通过用以连接用户的低端交换机等构成的接入层。

2. 3 层模型

层次化模型中最为经典的是 3 层模型。3 层模型主要将网络划分为核心层、汇聚层和接入层。

- 核心层：提供不同区域或者下层的高速连接和最优传输路径。
- 汇聚层：将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略。
- 接入层：为局域网接入广域网或者终端用户访问用户网络提供接入。

1)　核心层的设计要点

核心层是网络高速交换的主干，对整个网络的性能至关重要，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能够快速适应变化。在设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。

2)　汇聚层的设计要点

汇聚层处于核心层与接入层的分界点，应尽量将出于安全性原因对资源访问的控制、出于性能原因对通过核心层流量的控制等都在汇聚层实施。

为了保证层次化的特性，汇聚层应该向核心层隐藏接入层的详细信息。另外，汇聚层也会对接入层屏蔽网络其他部分的信息。为了保证核心层连接运行不同协议的区域，各种协议的转换都应在汇聚层完成。

3)　接入层的设计要点

接入层为用户提供了在本地网段访问应用系统的能力，接入层要解决相邻用户之间的互访需要，并且为这些访问提供足够的带宽。接入层还要负责一些用户管理功能和一些用户信息收集工作。

12.6.1.3　网络冗余设计

网络冗余设计通过设置双重网络元素来满足网络的可用性需求，冗余降低了网络的单点失效，其目的是重复设置网络组件，以避免单个组件的失效而导致应用失效。

在网络冗余设计中，对于通信线路常见的设计目标主要有两个：一个是作为备用路径；另一个是负载分担。

1. 备用路径

备用路径主要是为了提高网络的可用性。当一条路径或者多条路径出现故障时，为了保障网络的连通，网络中必须存在冗余的备用路径。备用路径由路由器、交换机等设备之间的独立备用链路组成。一般情况下，备用路径仅仅在主路径失效时投入使用。

2. 负载分担

负载分担是通过冗余的形式来提高网络的性能，是对备用路径方式的补充。负载分担是通过并行链路提供流量分担来提高性能，其主要的实现方法是利用两个或多个网络接口和路径来同时传递流量。

- 星型结构简单，管理方便，但冗余性不好，中心压力大，存在单点故障。
- 树型结构简单，中心压力小，但冗余性也不好，且有单点故障。
- 环型结构简单，管理方便，投资小，具有一定冗余度，但在网络存在差异较大的路径时，会引起网络时延的剧烈变化。

网状拓扑结构具有最小的时延、最高的冗余可靠性，但管理复杂，造价昂贵，常用于广域网。

12.6.1.4　广域网络技术

1. 传统的 PSTN 接入技术

PSTN 接入技术通过在客户计算机和远程的拨号服务器之间分别安装调制解调器，实现数字信号在模拟语音信道上的调制，通过公用电话网(PSTN)完成数据传输。PSTN 接入的传输速率低，目前常见的速率是 33.6kb/s 或者 56kb/s。

PSTN 接入主要使用两种协议，即 SLIP 和 PPP。SLIP(Serial Line Internet Protocol)只能为 TCP/IP 协议提供传输通道；PPP(Point to Point Protocol)协议可以为多种网络协议簇提供

传输通道，是应用最广泛的协议。设计 PPP 协议中，需要考虑口令认证机制，PPP 协议支持两种类型的认证机制：口令认证协议(RAP)和应答握手认证协议(CHAP)。

在设计 PSTN 接入时，需要在网络中添加远程访问服务器(RAS)，通常都是带有拨号服务的路由器。

2. 综合业务数据网

综合业务数据网(ISDN)是由地区电话服务提供商提供的数字数据传输业务。ISDN 提供的电路包括 64kb/s 的承载用户信息信道(B 道)和承载控制信息信道(D 道)，同时 ISDN 提供两种用户接口，即基本速率接口和基群速率接口。

3. xDSL 接入

数字用户线路(Digital Subscriber Line，DSL)技术是基于普通电话线的宽带接入技术。它可以在一根铜线上分别传送数据和语音信号，其中数据信号并不通过电话交换设备，并且不需要拨号，属于一直在线的专线上网方式。DSL 有许多模式，如 ADSL、RADSL、HDSL、SDSL 和 VDSL 等。通常把所有的 DSL 技术统称为 xDSL，“x”代表不同种类的 DSL 技术。

按数据传输的上、下行传输速率的不同，DSL 有对称和非对称传输两种模式。

1) HDSL

HDSL 的特点是在双绞铜线对上，采用有效的调制、数字均衡、回波抵消、信道编码等技术，均衡全部频段的线路损耗，消除噪声及串扰，使得用户环路的两对常规铜芯电缆能以 2.048Mb/s 的速率全双工地进行数据传输，中继距离达 3～5km。

HDSL 主要用于为企事业用户提供低成本的 2Mb/s 链路，包括会议电视线路、局域网互联、高速数据租用线、用户交换机的互联、ISDN 基群接入以及无线基站和移动交换机之间的连接等。

2) ADSL

ADSL(Asymmetrical Digital Subscriber Line)是一种非对称 DSL 技术，可在现有任意双绞线上传输，误码率低。ADSL 在一对铜线上，支持上行速率 512kb/s～1Mb/s，下行速率 1Mb/s～8Mb/s，有效传输距离为 3～5km。另外，在进行数据传输的同时还可以使用第三个通信信道，进行 4kHz 的语音传输。

现在比较成熟的 ADSL 标准有两种，即 G.DMT 和 G.Lite。G.DMT 是全速率的 ADSL 标准，支持 8Mb/s 及 1.5Mb/s 的高速下行及上行速率，但 G.DMT 要求用户端安装 POTS 分离器，比较复杂且价格昂贵；G.Lite 标准速率较低，下行速率为 1.5Mb/s，上行速率为 512kb/s，但省去了复杂的 POTS 分离器，成本较低且便于安装。G.DMT 较适用于小型办公室(SOHO)，而 G.Lite 则更适用于普通家庭。

3) VDSL

甚高比特率数字用户线(VDSL)可在较短的距离上获得极高的传输速率，是各种 DSL 技术中速度最快的一种，也是一种非对称技术。

4) SDSL

单线路数字用户线(SDSL)技术是对称的，上行通信与下行通信具有相同的传输速率(1.5Mb/s)。但 SDSL 技术还不成熟，标准也没有最终确立。

5) RADSL

RADSL(速率自适应数字用户线)技术采用非对称技术，能够在单对双绞线上以较低速率上载数据、以较高速率下载数据，并能保留原有语音通信。

4. HFC 接入

HFC(Hybrid Fiber-Coax)，混合光纤—同轴电缆，原意仅指采用光纤传输系统代替全同轴 CATV(公用天线电视和电缆电视)网络中的干线传输部分，而用户分配网络仍然保留同轴电缆结构。

HFC 网是综合应用模拟和数字传输技术、同轴电缆和光缆技术的宽带接入网络，它由光纤干线网和同轴电缆分配网通过光节点站结合而成，一般光纤干线网采用星型拓扑结构，同轴电缆分配网采用树型结构。HFC 网利用光纤传输的宽频带特性，用空余的频带来传输电信话音业务、高速数据业务和个人通信业务，充分利用光纤的频谱资源构成全业务的传输网络。

上行传输采用 DMT、QAM、DWMT 等抗干扰性的调制技术的电缆调制解调器(Cable Modem)的载频可调，上行速率可达 10Mb/s，下行速率可达 30Mb/s。当多个用户同时在一个子信道上向中心发送信息时，便造成冲突，使发送失败。因此要采用总线型网络中所采用的媒体访问控制(Medium Access Control，MAC)协议。根据采用的方案不同，前端中的主要设备有数字局端机(HDT)或基于 ATM 的局端机(ADT)或 ATM 和 STM 混合方式的局端机(ASDT)。

HFC 具有以下优势。

- 仅需一个光纤节点(FN)进行信号的转发、转换，节省了器件数量。
- 具有高达 1000MHz 的传输带宽。
- 可以传输电话语音业务、高速数据业务以及个人通信业务等多种业务。
- 比传统的 CATV 网络具有更高的资源利用率。

5. FTTx 接入

Fiber-To-The-x(FTTx，x = H for home，P for premises，C for curb and N for node or neighborhood)光纤接入，其中 FTTH 光纤到户，FTTP 光纤到驻地，FTTC 光纤到路边/小区，FTTN 光纤到节点。

FTTx 技术主要用于接入网络光纤化，范围从区域电信机房的局端设备到用户终端设备。局端设备为光线路终端(Optical Line Terminal，OLT)，用户终端设备为光网络单元(Optical Network Unit，ONU)或光网络终端(Optical Network Terminal，ONT)。根据光纤到用户的距离来分类，可分成光纤到交换箱(Fiber To The Cabinet，FTTCab)、光纤到路边(Fiber To The Curb，FTTC)、光纤到大楼(Fiber To The Building，FTTB)及光纤到户(Fiber To The Home，FTTH) 4 种服务形态。美国运营商 Verizon 将 FTTB 及 FTTH 合称为光纤到驻地(Fiber To The Premise，FTTP)。上述服务可统称 FTTx。

1) FTTC

FTTC 为目前最主要的服务形式，主要是为住宅区的用户提供服务，将 ONU 设备放置于路边机箱，利用 ONU 出来的同轴电缆传送 CATV 信号或双绞线传送电话及上网服务。

2) FTTB

FTTB 依服务对象区分为两种：一种是公寓大厦的用户服务；另一种是商业大楼的公司行号服务。两种皆将 ONU 设置在大楼的地下室配线箱处，只是公寓大厦的 ONU 是 FTTC 的延伸；而商业大楼是为了中大型企业单位。因此，必须提高传输的速率，以提供高速的数据、电子商务、视频会议等宽带服务。

3) FTTH

至于 FTTH，ITU 认为从光纤端头的光电转换器(或称为媒体转换器，MC)到用户桌面不超过 100m 的情况才是 FTTH。FTTH 将光纤的距离延伸到终端用户家中，使得家庭内能提供各种不同的宽带服务，如 VOD、在家购物、在家上课等，从而提供更多的商机。若搭配 WLAN 技术，将使得宽带与移动相结合，则可以达到未来宽带数字家庭的远景。

6. 宽带无线接入

宽带无线接入技术经过近几年的发展，已经形成了一定的产业规模。随着新的技术涌现，宽带无线接入的传输能力在不断增强，接口更加开放，技术的发展正经历从固定到移动的发展过程。现在，无线接入技术主要有 802.11 标准的无线局域网(WLAN)、802.16 标准的无线城域网(WMAN)和无线网格网(WMN)技术。

1) WLAN

由于 IEEE 802.11 的标准成功解决了空中接口兼容性问题，促进了无线局域网终端和接入点(AP)的互通，因此 WLAN 设备成本下降很快，应用也非常广泛。WLAN 在企业网中和公众网中都有应用，主要面向个人用户，公众热点一般部署在商旅人士经常出入的场所或数据业务需求较大的公共场合，如机场、会议中心、展览馆、宾馆等。

IEEE 802.11 只是 IEEE 最初制定的一个无线局域网标准，主要用于解决办公室局域网和校园网中用户与用户终端的无线接入问题，业务主要限于数据访问，速率最高只能达到 2Mb/s。由于它在速率和传输距离上都不能满足人们的需要，因此 IEEE 802.11 标准已被 IEEE 802.11b 所取代。

IEEE 802.11b 标准的优点在于：在不易接线或接线费用较高的区域中提供网络服务。灵活的工作组为需要经常更改网络配置的工作区降低了成本，所以它特别适用于小型办公环境和家庭网络。在室内环境中，针对不同的实际情况，IEEE 802.11b 可以有不同的典型解决方案。

(1) 对等解决方案。

对等解决方案是一种最简单的应用方案，每台 PC 只需安装一块无线网卡，即可相互访问。如果一台 PC 再安装一块有线网卡即可进行有线连接，无线网中其余 PC 可利用这台计算机作为网关，访问有线网络或共享打印机等设备。这是一种点对点的解决方案，网络中的计算机只能进行一对一的数据传输，不能同时进行多点访问。如果要实现有线局域网那样的互联功能，则必须借助接入点。

(2) 单接入点解决方案。

接入点相当于有线网络中的集线器。无线接入点可以连接周边的无线网络终端，形成星型网络结构，同时通过 10Base-T 端口与有线网络相连，这样整个无线网的终端都能访问有线网络的资源，并可通过路由器访问 Internet。

(3) 多接入点解决方案。

若网络规模较大以至于超过了单个接入点的覆盖半径，可以采用多个接入点分别与有线网络相联，从而形成以有线网络为主干的多接入点的无线网络，所有无线终端可以通过就近的接入点接入网络，访问整个网络的资源。

(4) 无线中继解决方案。

无线接入器还可以充当有线网络的延伸。比如在工厂车间中，车间具有一个网络接口连接有线网，而车间中许多信息点由于距离很远使得网络布线成本很高，还有一些信息点由于周边环境比较恶劣，无法进行布线。由于这些信息点的分布范围超出了单个接入点的覆盖半径，可以采用两个接入点实现无线中继，以扩大无线网络的覆盖范围。

(5) 无线冗余解决方案。

对于网络可靠性要求较高的应用环境，比如金融、证券等，接入点一旦失效，整个无线网络会瘫痪，将带来很大损失。因此，可以将两个接入点放置在同一位置，从而实现无线冗余备份的方案。

(6) 多蜂窝漫游工作方式。

在一个大楼中或者在很大的平面内部署无线网络时，可以布置多个接入点构成一套微蜂窝系统，这与移动电话的微蜂窝系统十分相似。微蜂窝系统允许一个用户在不同的接入点覆盖区域内任意漫游，随着位置的变换，信号会由一个接入点自动切换到另一个接入点。整个漫游过程对用户是透明的，虽然提供连接服务的接入点发生了切换，但对用户的服务却不会被中断。

2)　WMAN

当接入网技术特别是无线接入问题提出的时候，IEEE 802 委员会在 2002 年公布了宽带无线网络 802.16 标准，即无线城域网标准。在网络构成上，以 IEEE 802.16 系列标准为代表的宽带 WMAN 主要用于本地多点连接，既可将 802.11 系列无线接入互联网，也可连接企业与家庭环境至有线骨干线路。

3)　WMN

WMN 是移动 Ad hoc 网络的一种特殊形态，它的早期研究均源于移动 Ad Hoc 网络的研究与开发。它是一种高容量、高速率的分布式网络，不同于传统的无线网络，它可以看成是一种 WLAN 和 Ad hoc 网络的融合，且发挥了两者的优势。作为一种可以解决“最后一公里”瓶颈问题的新型网络结构，WMN 被写入了 IEEE 802.16 标准中。

12.6.1.5　广域网互联技术

1. 数字数据网

数字数据网(Digital Data Network，DDN)是利用数字信道传输数据信号的数据传输网。它的主要作用是向用户提供永久性和半永久性连接的数字数据传输信道，既可用于计算机之间的通信，也可用于传送数字化传真、数字话音、数字图像信号或其他数字化信号。

- 永久性连接的数字数据传输信道是指用户间建立固定连接，传输速率不变的独占带宽电路。
- 半永久性连接的数字数据传输信道对用户来说是非交换性的，但用户可提出申请，由网络管理人员对其提出的传输速率、传输数据的目的地和传输路由进行修改。

DDN 是一个全透明网络，能提供多种业务来满足各类用户的需求。

- 提供速率可以在一定范围内(200b/s～2Mb/s)任选的、信息量大、实时性强的中高速数据通信业务。
- 为分组交换网、公用计算机互联网等提供中继电路。
- 可提供点对点、一点对多点的业务，适用于金融证券公司、科研教育系统、政府部门租用 DDN 专线组建自己的专用网。
- 提供帧中继业务，扩大了 DDN 的业务范围。
- 提供语音、G3 传真、图像、智能用户电报等通信。
- 提供虚拟专用网业务。

利用 DDN 实现局域网互联时，必须借助于路由器和 DDN 提供的数据终端设备 DTU。DTU 实际上是 DDN 专线的调制解调器，直接和 DDN 通过专线连接。

虽然面临各种新型传输技术的挑战，但由于 DDN 可以为任何信号和传输协议提供透明传输，至今为止，DDN 仍在广域网互联技术应用中占据一席之地。

2. SDH

SDH(Synchronous Digital Hierarchy，同步数字系列)是一种将复接、线路传输及交换功能融为一体并由统一网管系统操作的综合信息传送网络，是美国贝尔通信技术研究所提出的同步光网络(SONET)。它可实现网络有效管理、实时业务监控、动态网络维护、不同厂商设备间的互通等多项功能，能大大提高网络资源利用率、降低管理及维护费用、实现灵活可靠和高效的网络运行与维护。

SDH 是主要的广域网互联技术，利用运营商的 SDH 网络实现互联，可以采用两种方式，即 IP over SDH 和 PDH 兼容方式。

1) IP over SDH

IP over SDH 是以 SDH 网络作为 IP 数据网络的物理传输网络，使用链路适配及成帧协议(PPP)对 IP 数据包进行封装，然后按字节同步的方式把封装后的 IP 数据包映射到 SDH 的同步净负荷封装中进行连续传输。IP over SDH 为 IP 网络设备提供的接口主要是 POS，该接口可以提供 STM-1 及其以上的传输速率。

2) PDH(准同步数字系列)兼容方式

SDH 提供了对传统 PDH 的兼容方式。这种方式在 SDH 中的最低速率同步传输模块 STM-1 中封装了 63 个 E1 信道，可以最多同时向 63 个用户提供 2Mb/s 的接入速率。

PDH 兼容方式可以提供两种方式的接口：传统 E1 接口和封装了多个 E1 信道的 CPOS，路由器通过一个 CPOS 接口接入 SDH 网络，并通过封装的 E1 信道连接多个远程站点。

3) MSTP

基于 SDH 的多业务传送平台(Multi-Service Transport Platform，MSTP)是指基于 SDH 平台实现 TDM、ATM、以太网等业务的接入、处理和传送，提供统一网管的多业务节点。

基于 SDH 的多业务传送节点除应具有标准 SDH 传送节点所具有的功能外，还具有以下主要功能特征。

- 具有 TDM 业务、ATM 业务或以太网业务的接入功能。
- 具有 TDM 业务、ATM 业务或以太网业务的传送功能，包括点到点的透明传送功能。

- 具有 ATM 业务或以太网业务的带宽统计复用功能。
- 具有 ATM 业务或以太网业务映射到 SDH 虚容器的指配功能。

MSTP 的实现基础是充分利用 SDH 技术对传输业务数据流提供保护恢复能力和较小的延时性能，并对网络业务支撑层加以改造，以适应多业务应用，实现对 2 层、3 层的数据智能支持。即将传送节点与各种业务节点融合在一起，构成业务层和传输层一体化的 SDH 业务节点，称为融合的网络节点或多业务节点，主要定位于网络边缘。

3. VPN 技术

1)　传统的 VPN 技术

虚拟专用网是通过公共网络实现远程用户或远程局域网之间的互联，主要采用隧道技术，让报文通过如 Internet 或其他商用网络等公共网络进行传输。

传统的 VPN 技术主要是基于数据安全传输的协议来完成，主要包括两个层次的数据安全传输协议：2 层协议和 3 层协议。

(1)　2 层协议主要是对传统拨号协议 PPP 的扩展，通过定义多协议跨越第二层点对点链接的一个封装机制，来整合多协议拨号服务至现有的因特网服务提供商，保证分散的远程客户端通过隧道方式经由 Internet 等网络访问企业内部网络。其典型协议为 L2TP。

(2)　3 层协议主要定义了在一种网络层协议上封装另一个协议的规范，可以在 VPN 寄生的网络上进行传递，使得各个 VPN 之间可以借助隧道进行通信。典型的 3 层协议包括 IPSec 和 GRE。

2)　MPLS VPN 技术

MPLS(Multi-Protocol Label Switching，多协议标记交换)是基于标记的 IP 路由选择方法，这些标记能被用来代表逐跳式或显式路由。MPLS 为每个 IP 数据包提供一个标记，将之和 IP 数据包封装于新的 MPLS 数据包，由此决定 IP 数据包的传输路径及优先顺序，而和 MPLS 兼容的路由器会在将 IP 数据包按相应路径转发之前仅读取该 MPLS 数据包的包头标记，无须再去读取每个 IP 数据包中的 IP 地址等信息，因此数据包的交换转发速度大大加快。

MPLS VPN 是一种基于 MPLS 技术的 IP-VPN，是在网络路由和交换设备上应用 MPLS 技术，简化核心路由器的路由选择方式，利用结合传统路由技术的标记交换实现的 IP 虚拟专用网络(IP-VPN)，可用来构造宽带的 Intranet、Extranet，满足多种灵活的业务需求。

12.6.1.6　安全运行与维护

网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。

网络安全体系设计的重点在于根据安全设计的基本原则，制定出网络各层次的安全策略和措施，然后确定出应选用什么样的网络安全系统产品。

1. 网络安全设计原则

尽管没有绝对安全的网络，但是，如果在网络方案设计之初就遵从一些合理的原则，

相应网络系统的安全和保密就更加有保障。从工程技术角度出发，在设计网络方案时，应该遵守以下原则。

(1) 网络信息系统安全与保密的“木桶原则”。

“木桶的最大容积取决于最短的一块木板”。强调对信息均衡、全面地进行安全保护。网络信息系统是一个复杂的计算机系统，它本身在物理上、操作上和管理上的种种漏洞构成了系统的安全脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的是“最易渗透原则”，即在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测(包括模拟攻击)，是设计网络安全系统的必要前提条件。

(2) 网络安全系统的整体性原则。

强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失。所以网络安全系统应该包括 3 种机制：安全防护机制、安全监测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全漏洞和安全威胁采取的相应防护措施，避免非法攻击的进行；安全监测机制是监测系统的运行情况，及时发现和制止对系统进行的各种攻击；安全恢复机制是在安全防护机制失效的情况下，进行应急处理和尽量、及时地恢复信息，减少攻击的破坏程度。

(3) 网络安全系统的有效性与实用性原则。

网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提。网络中的信息安全和信息利用是一对矛盾：一方面，为健全和弥补系统缺陷的漏洞，会采取多种技术手段和管理措施；另一方面，势必给系统的运行和用户的使用造成负担和麻烦，“越安全就意味着使用越不方便”。尤其在网络环境下，实时性要求很高的业务不能允许安全连接和安全处理造成的时延和数据扩张。如何在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户的记忆、存储工作和安全服务器的存储量、计算量，是一个亟待解决的问题。

(4) 网络安全系统的“等级性”原则。

良好的网络安全系统必然是分为不同级别的，包括对信息保密程度分级(绝密、机密、秘密、普密)，对用户操作权限分级(面向个人及面向群组)，对网络安全程度分级(安全子网和安全区域)，对系统实现结构的分级(应用层、网络层、链路层等)，从而针对不同级别的安全对象，提供全面的、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

(5) 设计为本原则。

强调安全与保密系统的设计应与网络设计相结合。由于安全与保密问题是一个相当复杂的问题，因此必须搞好设计才能保证安全性。

(6) 自主和可控性原则。

网络安全与保密问题关系着一个国家的主权和安全，所以网络安全产品不能依赖国外进口产品。

(7) 安全有价原则。

网络系统的设计是受经费限制的。因此在考虑安全问题解决方案时必须考虑性能价格的平衡，而且不同的网络系统所要求的安全侧重点各不相同，如国家政府首脑机关、国防

部门计算机网络系统安全侧重于存取控制强度，金融部门侧重于身份认证、审计、网络容错等功能，交通、民航侧重于网络容错等。因此必须有的放矢，具体问题具体分析，把有限的经费用在关键领域。

2. 网络信息安全设计与实施步骤

网络信息安全设计与实施步骤如下。

(1) 确定面临的各种攻击和风险。网络安全系统的设计和实现必须根据具体的系统和环境，考察、分析、评估、检测(包括模拟攻击)和确定系统存在的安全漏洞和安全威胁。

(2) 明确安全策略。安全策略是网络安全系统设计的目标和原则，是对应用系统完整的安全解决方案。安全策略要综合以下几方面优化确定。

① 系统整体安全性，由应用环境和用户需求决定，包括各个安全机制的子系统的安全目标和性能指标。

② 对原系统的运行造成的负荷和影响(如网络通信时延、数据扩展等)。

③ 便于网络管理人员进行控制、管理和配置。

④ 可扩展的编程接口，便于更新和升级。

⑤ 用户界面的友好性和使用方便性。

⑥ 投资总额和工程时间等。

(3) 建立安全模型。模型的建立可以使复杂的问题简化，更好地解决和安全策略有关的问题。安全模型包括网络安全系统的各个子系统。网络安全系统的设计和实现可以分为安全体制、网络安全连接和网络安全传输 3 部分。

① 安全体制，包括安全算法库、安全信息库和用户接口界面。

a. 安全算法库，包括私钥算法库、公钥算法库、Hash 函数库、密钥生成程序、随机数生成程序等安全处理算法。

b. 安全信息库，包括用户口令和密钥、安全管理参数及权限、系统当前运行状态等安全信息。

c. 用户接口界面，包括安全服务操作界面和安全信息管理界面等。

② 网络安全连接，包括安全协议和网络通信接口模块。

a. 安全协议，包括安全连接协议、身份验证协议、密钥分配协议等。

b. 网络通信接口模块。网络通信模块根据安全协议实现安全连接。一般用两种方式实现：安全服务和安全体制在应用层实现，经过安全处理后的加密信息送到网络层和数据链路层，进行透明的网络传输和交换，这种方式的优点是实现简单，不需要对现有系统做任何修改，用户投资数额较小；对现有的网络通信协议进行修改，在应用层和网络层之间加一个安全子层，实现安全处理和操作的自动性和透明性。

③ 网络安全传输，包括网络安全管理系统、网络安全支撑系统和网络安全传输系统。

a. 网络安全管理系统。安全管理系统安装于用户终端或网络节点上，是由若干可执行程序所组成的软件包，提供窗口化、交互化的“安全管理器”界面，由用户或网管人员配置、控制和管理数据信息的安全传输，兼容现有通信网络管理标准，实现安全功能。

b. 网络安全支撑系统。整个网络安全系统的可信方是由网络安全管理人员维护和管理的安全设备和安全信息的总和，包括密钥管理分配中心，负责身份密钥、公开钥和秘密钥

等密钥的生成、分发、管理和销毁；认证鉴别中心负责对数字签名等信息进行鉴别和裁决。网络安全支撑系统的物理和逻辑安全都是至关重要的，必须受到最严密和全面的保护。同时，也要防止管理人员内部的非法攻击和误操作，在必要的应用环境，可以引入秘密分享机制来解决这个问题。

c. 网络安全传输系统，包括防火墙、安全控制、流量控制、路由选择和审计报警等。

(4) 选择并实现安全服务。物理层的安全：物理层信息安全，主要防止物理通路的损坏、物理通路的窃听和对物理通路的攻击(干扰等)。

链路层的安全：链路层的网络安全需要保证通过网络链路传送的数据不被窃听。主要采用划分 VLAN(局域网)、加密通信(远程网)等手段。

网络层的安全：网络层的安全需要保证网络只给授权的客户使用授权的服务，保证网络路由正确，避免被拦截或监听。

操作系统的安全：操作系统安全要求保证客户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

应用平台的安全：应用平台指建立在网络系统之上的应用软件服务，如数据库服务器、电子邮件服务器、Web 服务器等。由于应用平台的系统非常复杂，通常采用多种技术来增强应用平台的安全性。

应用系统的安全：应用系统完成网络系统的最终目的——为用户服务。应用系统的安全与系统设计和实现关系密切。应用系统使用应用平台提供的安全服务来保证基本安全，如通信内容安全、通信双方的认证和审计等手段。

(5) 安全产品的选型测试。安全产品的选型测试工作严格按照企业信息与网络系统安全产品的功能规范要求，利用综合的技术手段，对参测产品在功能、性能与可用性等方面进行测试，为企业测试出符合功能规范的安全产品。测试工作原则上应该由中立组织进行；测试方法必须科学、准确、公正，必须有一定的技术手段；测试标准应该是国际标准、国家标准与企业信息和网络系统安全产品功能规范的综合；测试范围是产品的功能、性能与可用性。

12.6.2 典型例题分析

例 12-8 以下关于层次化网络设计的叙述中，错误的是<u>(64)</u>。(2017 年下半年真题 64)

A. 核心层实现数据分组从一个区域到另一个区域的高速转发

B. 接入层应提供丰富的接口和多条路径来缓解通信瓶颈

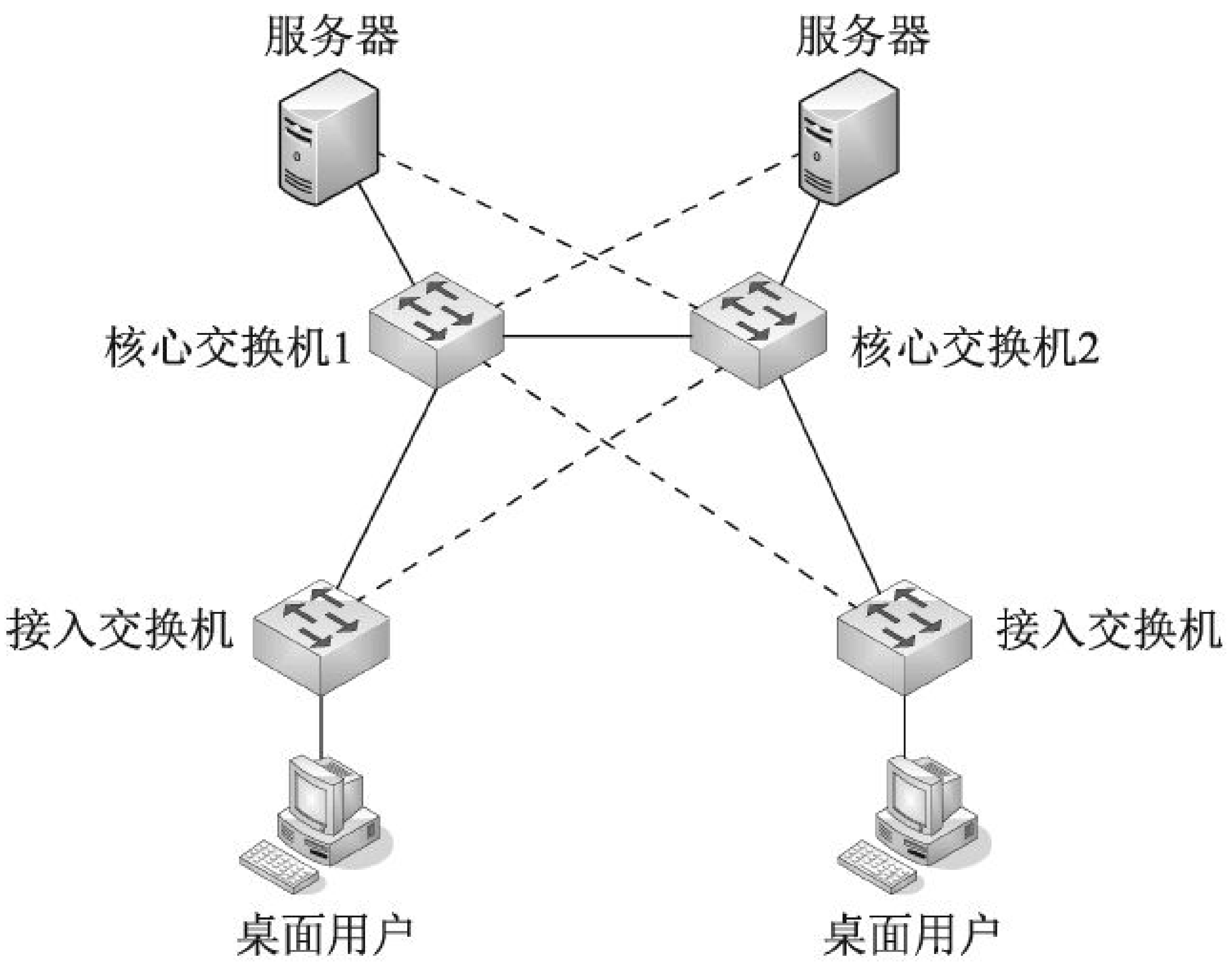
C. 汇聚层提供接入层之间的互访

D. 汇聚层通常进行资源的访问控制

解析：接入层为用户提供了在本地网段访问应用系统的能力，接入层要解决相邻用户直接的互访需要问题，并且为这些访问提供足够的带宽，并不考虑多路径选择。

答案：B

例 12-9 下图为某公司网络管理员规划的新办公大楼网络拓扑图，针对该网络规划，以下说法中不合理的是<u>(69)</u>。(2017 年上半年真题 69)



A. 核心交换机之间可以采用 VRRP、虚拟化等技术手段

B. 网络内各 VLAN 之间访问需要经过两台核心交换设备中的一台

C. 接入交换机多采用三层交换机

D. 网络拓扑结构可靠

解析：接入层是网络中直接面向用户连接或访问的部分，所以接入层应提供种类丰富、数量多的端口，从而能提供强大的接入功能，除此之外还要考虑接入的安全性问题。因此一般不采用三层交换机。

答案：C

例 12-10　在网络的分层设计模型中，对核心层工作规程的建议是__(69)__。(2016 年下半年真题 69)

A. 要进行数据压缩以提高链路利用率

B. 尽量避免使用访问控制列表以减少转发延迟

C. 可以允许最终用户直接访问

D. 尽量避免冗余连接

解析：核心层是网络高速交换的主干，对整个网络的性能至关重要，设计时应采用冗余组件设计，使其具备高可靠性，快速适应变化。设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的机制，以优化核心层获得低延迟和良好的可管理性。

答案：B

例 12-11　通过 HFC 网络实现宽带接入，用户端需要的设备是__(68)__，局端用于控制和管理用户的设备是__(69)__。(2015 年下半年真题 68、69)

(68)、(69)　A. Cable Modem　　B. ADSL Modem

C. OLT　　D. CMTS

解析：HFC 是将光缆敷设到小区，然后通过光电转换节点，利用有线电视(CATV)的总线式同轴电缆连接到用户，提供综合电信业务的技术。这种方式可以充分利用 CATV 原有的网络，建网快、造价低，逐渐成为最佳的接入方式之一。HFC 是由光纤干线网和同轴电缆分配网通过光节点站结合而成的，一般光纤干线网采用星型拓扑，同轴电缆分配网采用

树型结构。

在同轴电缆的技术方案中，用户端需要使用一个称为 Cable Modem(电缆调制解调器)的设备。它不单纯是一个调制解调器，还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身。它无须拨号，可提供随时在线的永远连接。其上行速率已达 10Mbps 以上，下行速率更高。

CMTS(电缆调制解调器终端系统)是管理控制 Cable Modem 的设备，其配置可通过 Console 接口或以太网接口完成。其配置内容主要有：下行频率、下行调制方式、下行电平等。

答案：(68) A (69) D

例 12-12 以下关于层次化局域网模型中核心层的叙述，正确的是__(70)__。(2015 年下半年真题 70)

A. 为了保障安全性，对分组要进行有效性检查

B. 将分组从一个区域高速地转发到另一个区域

C. 由多台 2、3 层交换机组成

D. 提供多条路径来缓解通信瓶颈

解析：层次化模型中最为经典的是 3 层模型，主要将网络划分为核心层、汇聚层和接入层。核心层一般由经过可用性和性能优化的高端路由器和交换机组成，提供不同区域或者下层的高速连接和最优传送路径；汇聚层由用于实现策略的路由器或者交换机构成，将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略；接入层由连接用户的低端交换机构成，为局域网接入广域网或者终端用户访问网络提供接入。

答案：B

12.6.3 同步练习

1. 下列关于网络汇聚层的描述中，正确的是________。

A. 要负责收集用户信息，例如用户 IP 地址、访问日志等

B. 实现资源访问控制和流量控制等功能

C. 将分组从一个区域高速地转发到另一个区域

D. 提供一部分管理功能，例如认证和计费管理等

2. 通过 ADSL 访问 Internet，在用户端通过__(1)__和 ADSL Modem 连接 PC，在 ISP 端通过__(2)__设备连接因特网。

(1)、(2) A. 分离器 B. 电话交换机 C. DSLAM D. IP 路由器

3. 数字用户线(DSL)是基于普通电话线的宽带接入技术，可以在铜质双绞线上同时传送数据和话音信号。下列选项中数据速率最高的 DSL 标准是______。

A. ADSL B. VDSL C. HDSL D. RADSL

4. 利用 SDH 实现广域网互联，如果用户需要的数据传输速率较小，可以用准同步数字系列(PDH)兼容的传输方式在每个 STM-1 帧中封装_______个 E1 信道。

A. 4 B. 63 C. 255 D. 1023

5. 下列关于网络核心层的描述中，正确的是______。

A. 为了保障安全性，应该对分组进行尽可能多的处理
B. 将数据分组从一个区域高速地转发到另一个区域
C. 由多台 2、3 层交换机组成
D. 提供多条路径来缓解通信瓶颈

6. 以下关于网络安全设计原则的说法，错误的是______。
A. 充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件
B. 强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失
C. 考虑安全问题解决方案时无须考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合
D. 网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提

7. 在层次化网络设计中，______不是分布层/接入层交换机的选型策略。
A. 提供多种固定端口数量搭配供组网选择，可堆叠、易扩展，以便由于信息点的增加而进行扩容
B. 在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单
C. 具备一定的网络服务质量和控制能力以及端到端的 QoS
D. 具备高速的数据转发能力

12.6.4　同步练习参考答案

1. D　　2. (1) A　(2) C　　3. B　　4. B　　5. B
6. C　　7. D

12.7　网络故障诊断

12.7.1　考点辅导

12.7.1.1　网络故障诊断概述

网络故障诊断是以网络原理、网络配置和网络运行的知识为基础，从故障现象出发，以网络诊断工具为手段获取诊断信息、确定网络故障点、查找问题的根源、排除故障、恢复网络正常运行的软件或者硬件。

1. 引发网络故障的原因

引发网络故障的原因如下。

- 物理层中物理设备相互连接失败或者硬件及线路本身的问题。
- 数据链路层的网络设备的接口配置问题。
- 网络层网络协议配置或操作错误。
- 传输层的设备性能或通信拥塞问题。
- 上 3 层或网络应用程序错误。

2. 排除网络故障的流程

在排除网络中出现的故障时，使用系统的方法往往更为有效。系统的方法流程如下：定义特定的故障现象，根据特定现象推断出可能发生故障的所有潜在问题，直到故障现象不再出现为止。图 12-6 给出了一般故障排除模型的处理流程。

注意：在网络故障的排除过程中，最为关键的是确保当前掌握的信息及资料是最新的。

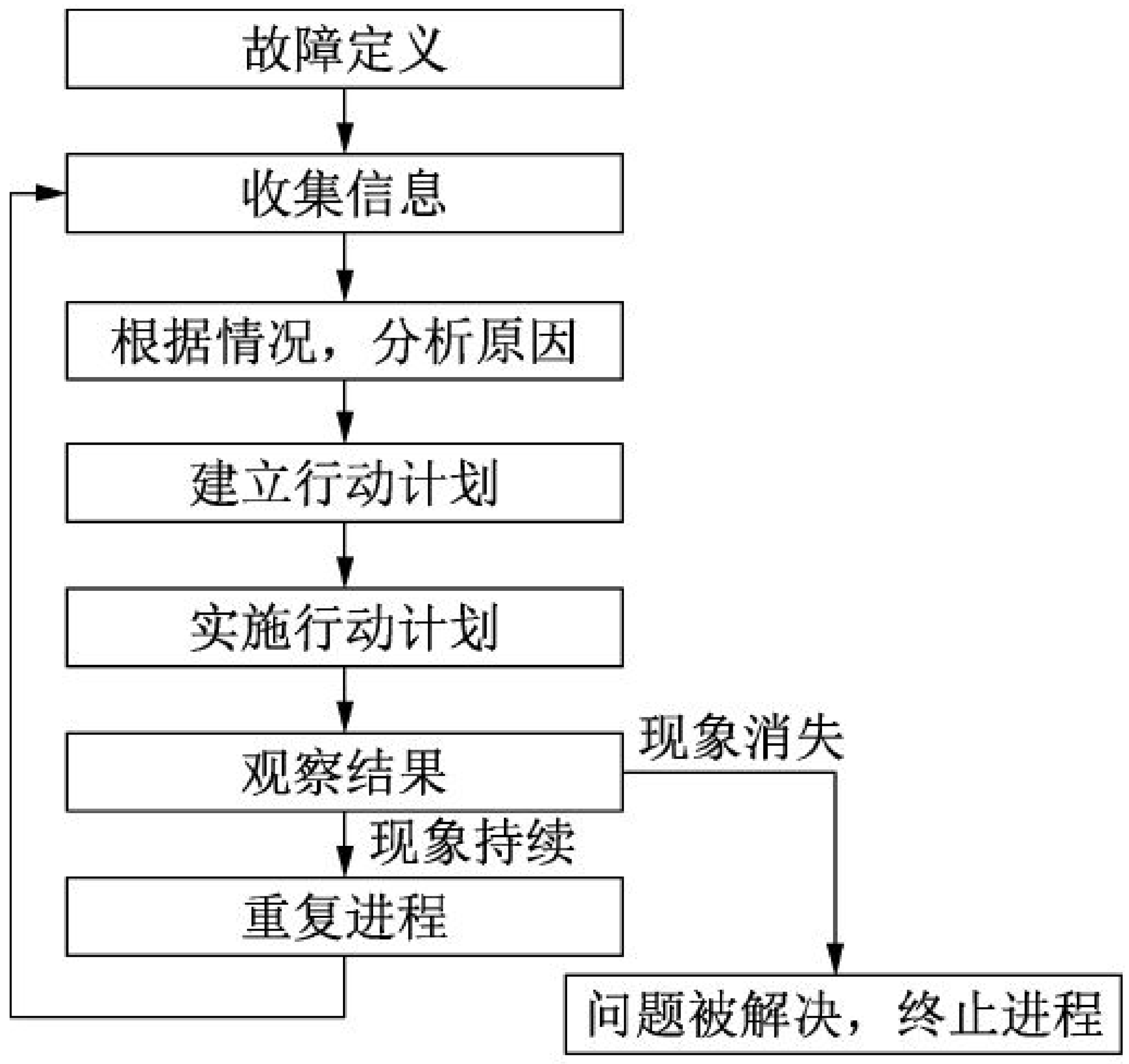


图 12-6　一般性故障问题的解决模型

12.7.1.2　网络故障的排除工具

排除网络故障常用的工具有 3 类：设备或系统诊断命令、网络管理工具以及专业故障排除工具。

1. 设备或系统诊断命令

设备或系统诊断命令有如下几种。

- show：用于监视系统的安装情况与网络的正常运行情况，也可用于对故障区域的定位。
- debug：帮助分析协议和配置问题。
- ping：用于检查网络上不同设备之间的连通性。
- trace：可以用于确定数据包从一个设备到另一个设备直至目的地的过程中所经历的路径。

2. 网络管理工具

Cisco Works、HP OpenView 等网络管理工具都含有监测以及故障排除功能。

3. 专业故障排除工具

专业故障排除工具有以下几种。

(1) 欧姆表、数字万用表及电缆测试器。其中，电缆测试器可用于检测电缆的物理连通性。

(2) 时域反射器与光时域反射器。时域反射器(TDR)能够快速地定位金属电缆中的短

路、断路、压接、扭结、阻抗不匹配等问题；光时域反射器(OTDR)可以精确地测量光纤的长度、定位光纤的断裂处、测试光纤的信号衰减、测试接头或连接器造成的损耗。

(3) 断接盒、智能测试盘和位/数据块错误测试器。这类设备可以检测数据线路的状态，捕获并分析数据，诊断数据通信系统中常见的故障。

(4) 网络检测器。该设备可以收集诸如数据包长度、数据包数量、错误数据包的数据、连接的总体利用率、主机与 MAC 地址的数量等信息。网络检测器不会对数据帧中的内容进行解码。

(5) 网络分析仪。它能够对不同协议层的通信数据进行解码，以便以阅读的缩略语或概述形式表示出来，详细表示哪个层被调用，以及每个字节或者字节内容起什么作用。

12.7.1.3　网络故障的分层诊断

1. 物理层及其诊断

物理层的故障主要表现在设备的物理连接方式是否恰当，连接电缆是否正确。确定路由器端口物理连接是否完好的最佳方式是使用 show interface 命令。

2. 数据链路层及其诊断

查找和排除数据链路层的故障，需要查看路由器的配置，检查连接端口共享同一数据链路层的封装情况。

3. 网络层及其诊断

排除网络层故障的基本方式是：沿着从源到目标的路径查看路由器的路由表，同时检查路由器接口的 IP 地址。

4. 应用层及其诊断

排除应用层故障的基本方法是：首先可在服务器上检查配置，测试服务器是否正常运行，如果服务器没有问题再检查应用客户端是否正确配置。

12.7.2　典型例题分析

例 12-13　当传输介质出现老化、破损、介质规格不匹配时会导致物理接口处于 DOWN 状态，常使用__(47)__命令检查光纤模块状态、参数是否正常。(2017 年上半年真题 47)

A. virtual-cable-test　　B. display transceiver interface

C. display device　　D. display interface

解析：display transceiver interface 用来显示设备接口上的光模块信息。

答案：B

例 12-14　在网络运行中，发现设备 CPU 长时间占用过高，经检查发现下图中的“Number of topology changes”值频繁变化，可初步判断该故障由__(48)__导致，可能的原因是__(49)__。(2017 年上半年真题 48、49)

```
<Switch>display stp topology-change
                    CIST topology change information
  Number of topology changes                     :35
  Time since last topology change                :0 days 1h:7m:30s
  Topology change initiator(notified)            :GigabitEthernet2/0/6
  Topology change last received from             :101b-5498-d3e0
  Number of generated topologychange traps:      38
  Number of suppressed topologychange traps:     8
```

(48) A. 硬件故障　　B. 网络攻击　　C. 网络震荡　　D. 网络环路

(49) A. 网络上某个端口链路属性频繁变化

B. 广播风暴造成大量协议报文

C. 设备受到 DHCP 报文攻击

D. 在部分硬件故障时会上报大量中断

解析：拓扑信息变动频繁，可以推测产生了网络震荡。出现网络震荡时，网络频繁变动，设备忙于处理网络切换事件，导致 CPU 占用率高。

答案：(48) C　(49) A

例 12-15　在 SwitchA 上 Ping SwitchB 的地址 192.168.1.100 不通。通过步骤①到④解决了该故障，该故障产生的原因是__(50)__。(2017 年上半年真题 50)

① 使用 display port vlan 命令查看 SwitchA 和 SwitchB 接口配置。

② 使用 display ip interface brief 命令查看 SwitchA 和 SwitchB 接口配置。

③ 使用 portlink-typetrunk 命令修改 SwitchB 配置。

④ 使用 ping192.168.1.100 检查，故障排除。

A. SwitchB 接口 VLAN 不正确　　B. SwitchB 的接口状态为 DOWN

C. SwitchB 链路类型配置错误　　D. SwitchB 对接收到的 ICMP 报文丢弃

解析：由步骤 3 可知交换机 B 配置做出了修改，说明两边链路封装不一致。

答案：C

例 12-16　在对网络设备巡检中，检测到交换机端口有大量的 CRC 错包，结合错包呈现出不断上涨的趋势，下面故障原因中，不可能的是__(70)__。(2017 年上半年真题 70)

```
[Switch-GigabitEthernet0/0/1]display this interface
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
Unicast       :     984907,Multicast    :     0
Broadcast     :     0,Jumbo             :     0
CRC           :     4782,Giants         :     0
Jabbers       :     0,Throttles         :     0
Runts         :     0,DropEvents        :     0
```

A. 端口状态异常　　B. 物理链路故障　　C. 电磁干扰　　D. 病毒攻击

解析：出现大量的 CRC 错包，说明是网络底层的相应故障，不可能是病毒攻击。

答案：D

12.7.3　同步练习

如果希望别的计算机不能通过 ping 命令测试服务器的连通情况，可以__(1)__。如果希望通过默认的 Telnet 端口连接服务器，则下面对防火墙的配置正确的是__(2)__。

(1) A. 删除服务器中的 ping.exe 文件　　B. 删除服务器中的 cmd.exe 文件

　　C. 关闭服务器中的 ICMP 端口　　D. 关闭服务器中的 Net Logon 服务

(2) A.

B.

C.

D.

12.7.4　同步练习参考答案

(1) C　(2) A

12.8　网络规划案例

12.8.1　考点辅导

本节将以具体实例的形式，来介绍网络规划的具体方法。

12.8.2 典型例题分析

例 12-17 网络拓扑设计对网络的影响主要表现在________。

①网络性能 ②系统可靠性 ③出口带宽 ④网络协议

A. ①② B. ①②③ C. ③④ D. ①②④

解析：网络拓扑设计对网络的影响主要表现在网络性能、系统可靠性和网络协议。

答案：D

12.8.3 同步练习

以下关于直通交换的叙述中，正确的是________。

A. 比存储转发交换速率要慢

B. 存在坏帧传播的风险

C. 接收到帧后简单存储，进行 CRC 校验后快速转发

D. 采用软件方式查找站点转发

12.8.4 同步练习参考答案

B

12.9 本 章 小 结

本章知识点在 2014 年的新大纲中改动不多，主要是知识点的明确化、具体化。

本章要求考生掌握网络规划的相关知识，包括网络系统的需求分析、网络系统的设计、通信子网的设计、资源子网的设计、网络系统的构建和测试。

本章相关知识点在历次考试中分布相对集中，分值在 10 左右，是考试的重点。根据往年的考题，本章前几节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

12.10 达标训练题及参考答案

12.10.1 达标训练题

1. 网络系统生命周期可以划分为 5 个阶段，实施这 5 个阶段的合理顺序是______。

   A. 需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段

   B. 需求规范、逻辑网络设计、通信规范、物理网络设计、实施阶段

C. 通信规范、物理网络设计、需求规范、逻辑网络设计、实施阶段

D. 通信规范、需求规范、逻辑网络设计、物理网络设计、实施阶段

2. 网络系统设计过程中，物理网络设计阶段的任务是______。

A. 依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B. 分析现有网络和新网络的各类资源分布，掌握网络的状态

C. 根据需求规范和通信规范，实施资源分配的安全规划

D. 理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

3. 在网络层采用分层编址方案的好处是________。

A. 减少了路由表的长度　　B. 自动协商数据速率

C. 更有效地使用 MAC 地址　　D. 可以选用更复杂的路由选择算法

4. 下列关于网络核心层的描述中，正确的是________。

A. 为了保障安全性，应该对分组进行尽可能多的处理

B. 将数据分组从一个区域高速地转发到另一个区域

C. 由多台 2、3 层交换机组成

D. 提供多条路径来缓解通信瓶颈

12.10.2　参考答案

1. A　2. A　3. A　4. B

第 13 章　计算机基础知识

大纲要求：

- 计算机组成、存储器、输入/输出结构和设备、中断、DMA、通道、SCSI、I/O 接口、输入和输出设备类型和特征。
- 操作系统的基本概念，处理机管理、存储管理、设备管理、文件管理、作业管理，包括进程的状态及转换、进程调度算法、死锁、存储管理方案、文件管理、作业调度算法，系统管理。
- 需求分析和设计、测试评审方法、项目管理基础知识、系统维护。
- 标准，安全性标准，标准化组织，全球信息化趋势、国家信息化战略、企业信息化战略和策略、互联网相关的法律和法规知识，个人信息保护规则，远程教育、电子商务、电子政务等基础知识，企业信息化资源管理基础知识。

13.1　计算机硬件基础

13.1.1　考点辅导

计算机硬件通常包括运算器、控制器、主存储器、输入设备和输出设备五大部件。其中把运算器和控制器合称为中央处理器，简称 CPU；把中央处理器和主存储器合称为主机。运算器是对数据进行加工处理的部件，它主要完成算术和逻辑运算。控制器的主要功能是从主存中取出指令，并指出下一条指令在主存中的位置。取出的指令经指令寄存器送往指令译码器，经过对指令的分析发出相应的控制和定时信息，控制计算机的各个部件有条不紊地工作，以完成指令所规定的操作。存储器是计算机系统中的记忆设备，用来存放程序、原始数据、中间结果及最终结果。输入设备的作用是把程序和原始数据转换成计算机中表示的二进制数，输入到计算机的主存中。输出设备的作用是把运算处理结果按照人们所要求的形式输出到外部存储介质上。

13.1.1.1　计算机中数据的表示

1. 机器数和码制

各种数据在计算机中的表示形式称为机器数，其特点是采用二进制计数制，数的符号用 0、1 表示，小数点则隐含表示而不占位置。真值是机器数所代表的实际数值。

机器数有无符号数和带符号数两种。无符号数表示正数，没有符号位。对无符号数，若约定小数点的位置在机器数的最低位之后，则是纯整数；若约定小数点的位置在最高位之前，则是纯小数。带符号数的最高位是符号位，其余位表示数值，同样，若约定小数点的位置在机器数的最低位之后，则是纯整数；若约定小数点的位置在最高数值位之前(符号

位之后)，则是纯小数。

为方便运算，带符号的机器数可采用原码、反码和补码等不同的编码方法，这些编码方法称为码制。

1)　原码表示法

数值 X 的源码记为$[X]_{原}$，最高位为符号位，表示该数的符号，“0”表示正数，“1”表示负数，而数值部分仍保留着其真值的特征。

2)　反码表示法

反码的符号的表示法与原码相同。正数的反码与正数的原码形式相同；负数的反码符号位仍为 1，数值部分通过将负数原码的数值部分各位取反(0 变 1，1 变 0)得到。

3)　补码表示法

正数的补码与原码相同；负数的补码是反码末位+1(丢弃最高位向上的进位)，它是最适合进行数字加减运算的数字编码。

2. 定点数和浮点数

实际处理的数既有整数部分又有小数部分，根据小数点位置是否固定，有两种表示格式：定点格式和浮点格式。

1)　定点表示法

定点表示法就是约定小数点的位置固定不变。小数点可以约定在数中的任何位置上，通常将小数点固定在符号位之后或整个数据的末位之后，也即将数据表示成纯小数或纯整数。定点数的运算规则比较简单，但不适宜对数值范围变化比较大的数据进行运算。

2)　浮点表示法

浮点表示法就是小数点的位置不固定，可根据需要左右浮动。在计算机中，一个任意进制数 N，其浮点数的真值为

$$N = \pm R^{E} M$$

式中，M 为尾数；E 为指数；R 为基数，一般取 2、8、16。一旦机器定义好基数值，就不能再改变。因此，在浮点数表示中基数不出现，是隐含的。

3. 校验码

通常使用校验码的方法来检测传送的数据是否出错。基本思想是把数据可能出现的编码分为两类，即合法编码和错误编码。合法编码用于传送数据，错误编码是不允许在数据中出现的编码。

校验码中有一个重要概念是码距。码距是指一个编码系统中任意两个合法编码之间至少有多少个二进制位不同。

1)　奇偶校验码

奇偶检验通过在编码中增加一位来使编码中 1 的个数为奇数(奇校验)或者为偶数(偶校验)，从而使码距变为 2。

2)　海明码

海明码是利用奇偶性来检错和校验的方法。其构成方法是：在数据位之间插入 k 个校验位，通过扩大码距来实现检错和纠错。

3)　循环冗余校验码

循环冗余校验码(CRC)由两部分组成，左边为信息码(数据)，右边为校验码。若 CRC 的字长为 n，信息码占 k 位，则校验码就占 $n-k$ 位。校验码是由信息码产生的，校验位越长，校验能力就越强。在求 CRC 时，采用的是模 2 运算。

13.1.1.2　中央处理器

中央处理器，即 CPU，是运算器和控制器的合称。

1. CPU 的功能

CPU 的功能如下。

(1)　程序控制。CPU 通过执行指令来控制程序的执行顺序。

(2)　操作控制。一条指令功能的实现需要若干操作信号来完成，CPU 产生每条指令的操作信号并将其送往不同的部件，控制相应部件的操作。

(3)　时序控制。CPU 通过时序电路产生的时钟信号进行定时，以控制各种操作按指定时序进行。

(4)　数据处理。完成对数据的加工处理。

2. CPU 的组成

1)　运算器

运算器主要完成算术运算、逻辑运算和移位操作，主要部件有算术逻辑单元(ALU)、累加器(ACC)、标志寄存器、寄存器组、多路转换器和数据总线等。

2)　控制器

控制器实现指令的读入、寄存、译码和在执行过程有序地发出控制信号。控制器主要由指令寄存器(IR)、程序计数器(PC)、指令译码器、状态/条件寄存器、时序产生器、微操作信号发生器组成。

3)　寄存器

寄存器用于暂存寻址和计算过程的信息。CPU 中的寄存器通常分为存放数据的寄存器、存放地址的寄存器、存放控制信息的寄存器、存放状态信息的寄存器和其他寄存器等类型。

3. 流水线技术

流水线技术把 CPU 的一个操作进一步分解成多个可以单独处理的子操作(如取指令、指令译码、取操作数、执行)，使每个子操作在一个专门的硬件站上执行，这样一个操作需要顺序地经过流水线中多个站的处理才能完成。在执行的过程中，前后连续的几个操作可以依次流入流水线中，在各个站间重叠执行。其工作原理如图 13-1 所示。

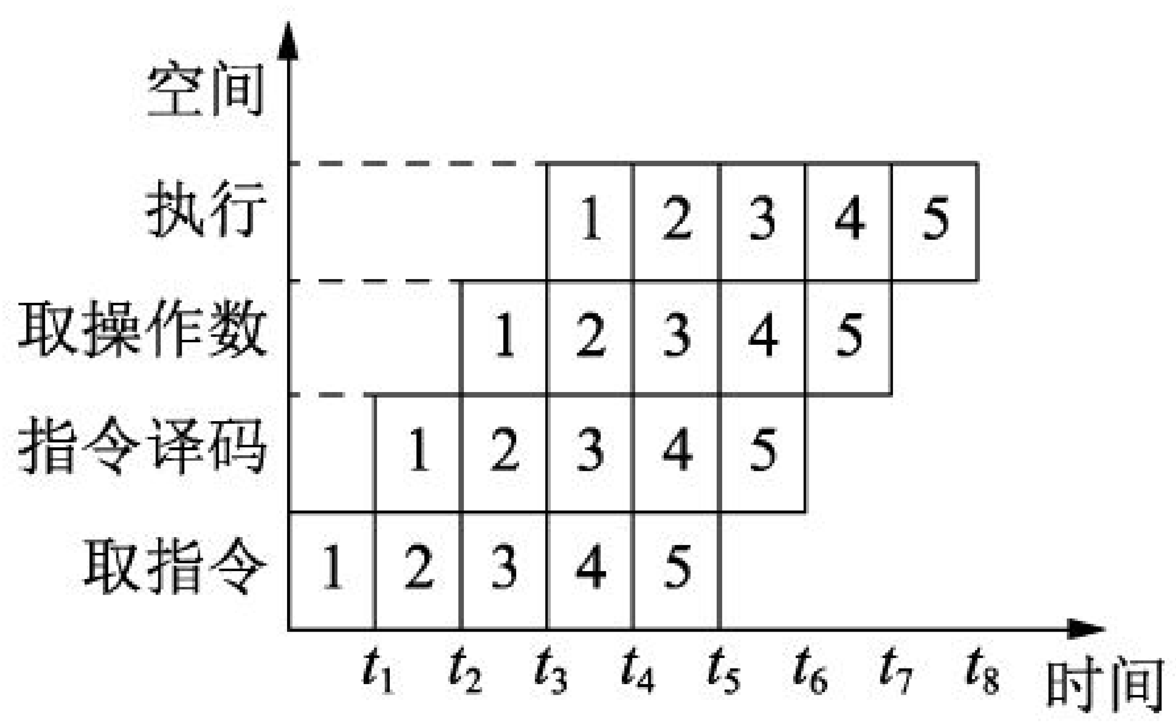


图 13-1　流水线技术

设某流水线技术分为 n 个基本操作，操作时间分别是 $\Delta t_i (i=1,2,\cdots,n)$。

(1) 操作周期。取决于基本操作时间最长的一个，即操作周期为

$$\Delta t = \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

(2) 吞吐率。流水线的吞吐率为

$$p = 1/\Delta t = 1/\max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

(3) 流水线的建立时间。即第一条指令完成的时间，即

$$T_1 = n \times \Delta t = n \times \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

(4) 执行 m 条指令时间，即

$$T = n \times \Delta t + (m-1) \times \Delta t = (n+m-1) \times \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

或

$$T = \sum_{i=1}^{n} \Delta t_i + (m-1) \times \Delta t = \sum_{i=1}^{n} \Delta t_i + (m-1) \times \max\{\Delta t_1, \Delta t_2, \cdots, \Delta t_i\}$$

13.1.1.3　存储系统

1. 主存储器

主存储器简称内存或主存，用来存放当前正在使用或随时要使用的数据和程序，CPU 可直接访问。主存一般由 RAM 和 ROM 两种工作方式的存储器组成，其绝大部分存储空间由 RAM 构成。

主存储器的性能指标包括以下几个方面。

(1) 存储容量。每个内存储单元都有一个地址，对内存的读、写操作都要给出地址来选择具体单元。在微机系统中内存是以字节作为一个单元的。在不同字长的系统中，一次可以对 2 个、4 个或 8 个单元进行访问。存储容量用字数或字节数(B)来表示，如 64KB、512KB、10MB。

(2) 存取时间。存取时间指从启动一次存储器操作到完成该操作所经历的时间。

(3) 存储周期。存储周期指连续启动两次独立的存储器操作(如连续两次读操作)所需间隔的最小时间。通常，存储周期略大于存储时间，其时间单位为 ns。

(4) 存储器带宽。存储器带宽指每秒钟能访问的 bit 数，记作 B_m。设每个存取周期存取数据位为 W_b，则 $B_m=W_b/T_m$。

2. 存储器的构成

由于存储器芯片的容量是有限的，在字数或字长方面与实际存储器的要求都有很大差距，可以通过字向和位向两方面进行扩充。假设一个存储器的容量为 $M\times N$ 位，若使用 $m\times n$ 位的芯片($m\leqslant M$，$n\leqslant N$)，此时共需要$(M/m)\times(N/n)$个存储器芯片。

3. 相联存储器

相联存储器(CAM)是一种按内容寻址的存储器。其工作原理就是把数据或数据的某一部分作为关键字，将该关键字与存储器中的每一单元进行比较，找出存储器中所有与关键字相同的数据。

4. Cache

Cache 即高速缓冲存储器，是为了解决 CPU 和主存之间速度匹配问题而设置的。它是介于 CPU 和主存之间的小容量存储器，存取速度比主存快。其改善系统性能的依据是程序的局部性原理。

- Cache 主要由两部分组成，即控制部分和存储器部分。
- Cache 存储器部分用来存放主存的部分副本。
- 控制部分的功能是判断 CPU 要访问的信息是否在 Cache 存储器中，若在即为命中，若不在则没有命中。

5. 性能分析

(1) 命中率。命中率指在 Cache 中访问到信息的概率，一般用模拟实验的方法得到。选择一组有代表性的程序，在程序执行过程中分别统计对 Cache 的访问次数 N_1 和对主存的访问次数 N_2，则 Cache 的命中率为 $H = N_1/(N_1 + N_2)$。

(2) 平均实际存取时间。平均实际存取时间可以用 Cache 和主存的访问周期 T_1、T_2 和命中率 H 来表示：$T = H \cdot T_1 + (1-H) \cdot T_2$。当命中率 $H \to 1$ 时，$T \to T_1$，即平均实际存取时间 T 接近于速度比较快的 Cache 的访问周期 T_1。

(3) 访问效率。访问效率为 $e = T_1/T$。

6. 地址映像

当 CPU 访问内存时，用的是访问主存的地址，由该地址变为访问 Cache 的地址称为“地址变换”。变换过程采用硬件实现，以达到快速访问的目的。地址映像方式有全相联方式、直接方式和组相联方式。

7. 磁盘存储器

磁盘存储器是外存中最常用的存储介质，存取速度较快且具有较大的存储容量。分为软盘存储器和硬盘存储器。

13.1.1.4 输入/输出系统

1. I/O 接口

I/O 接口又称为界面，指两个相对独立子系统之间的相连部分。用于连接主机和 I/O 设备的这个转换机构就是 I/O 接口电路。

接口有多种分类方法。

(1) 按数据的传送格式分为并行接口和串行接口。

(2) 按主机访问 I/O 设备的控制方式，可分为程序查询接口、中断接口、DMA 接口以及通道控制器、I/O 处理机等。

(3) 按时序控制方式可分为同步接口和异步接口。

2. 接口的控制方式

接口的控制方式有如下几种。

1) 直接程序控制方式

直接程序控制方式有以下两种。

(1)　程序查询方式。在这种方式下，CPU 通过执行程序查询外设的状态，判断外设是否准备好进行数据传送。

(2)　立即程序传送方式。在这种方式下，I/O 接口总是准备好接收来自主机的数据，或随时准备向主机输入数据，CPU 无须查看接口的状态，而直接执行输入/输出指令进行数据传送。这种方式又称为无条件传送或同步传送。

2)　中断方式

中断方式是指当出现来自系统外部、机器内部，甚至处理机本身的任何例外时，CPU 暂停执行现行程序，转去处理这些事件，等处理完成后再返回来继续执行原先的程序。

3)　DMA 方式

DMA(直接存储器存取)方式不是用软件而是采用一个专门的控制器来控制内存与外设之间的数据交流，无须 CPU 介入，可大大提高 CPU 的工作效率。

4)　I/O 通道方式

通道又称输入/输出处理器(IOP)，目的是使 CPU 摆脱繁重的输入输出负担和共享输入输出接口，多用于大型计算机系统中。根据多台外围设备共享通道的不同情况，可将通道分为 3 种类型：字节多路通道、选择通道和数组多路通道。

13.1.1.5　总线系统

1. 总线的定义与分类

总线是连接多个设备的信息传送通道，是一组信号线。一般可分为芯片内总线、元件级总线、内总线、外总线(又称通信总线)。

1)　内总线

内总线又称系统总线，是计算机各组成部分(CPU、内存和外设接口)间的连接。系统总线按功能可分为 3 类，即地址总线、数据总线、控制总线。

常见的内总线标准有如下几种。

- ISA(Industry Standard Architecture)总线：数据线 16 位，地址线 24 位。
- EISA(Enhanced Industry Standard Architecture)总线：EISA 总线是 ISA 总线的扩展，现用在服务器上。数据线 32 位。与 ISA 总线兼容。
- PCI(Peripheral Computer Interconnect)总线：目前微型机上广泛采用内总线。PCI 总线的工作与处理机的工作是并行的。PCI 总线上的设备可即插即用。

2)　外总线

外总线又称通信总线，是计算机对外的接口，可直接与相应的外设连接或与其他计算机相连接。常见的外总线标准有以下几种。

- 串行总线接口(RS-232)：是国际通用的一种串行通信接口标准。
- SCSI(Small Computer System Interface)总线：是一条并行外部总线，广泛用于连接软硬磁盘、光盘、扫描仪等。
- 通用串行总线(Universal Serial Bus，USB)：USB 接口提供电源，最大数据传输率为 12Mb/s，支持即插即用功能。
- IEEE 1394(Firewire)：由 6 条信号线组成，可连接设备数多，传输速度快，支持即插即用。

2. 总线的指标

总线的指标有以下几种。

(1) 总线宽度。一次可以传输数据的位数，S100 为 8 位，ISA 为 16 位，EISA 为 32 位，PCI-2 可达 64 位。总线宽度不会超过微处理器外部数据总线的宽度。

(2) 总线工作频率。总线信号中有一个 CLK 时钟信号，CLK 越高每秒钟传输的数据量越大。ISA、EISA 为 8MHz，PCI 为 33.3MHz，PCI-2 为 66.6MHz。

(3) 单个数据传输周期。不同的传输方式，每个数据传输所用 CLK 周期数不同。ISA 用 2 个周期，PCI 用 1 个周期。这决定总线最高数据传输率。

13.1.1.6 指令系统

1. 指令

指令是指挥计算机完成各种操作的基本命令。

(1) 指令格式。计算机的指令由操作码字段和操作数字段两部分组成。

(2) 指令长度。指令长度有固定长度的和可变长度的两种。有些 RISC 的指令是固定长度的，但目前多数计算机系统的指令是可变长度的。指令长度通常取 8 的倍数。

(3) 指令种类。指令有数据传送指令、算术运算指令、位运算指令、程序流程控制指令、串操作指令、处理器控制指令等类型。

2. 寻址方式

寻址方式有以下几种。

(1) 立即寻址。立即寻址是指操作数作为指令的一部分而直接写在指令中，这种操作数称为立即数。

(2) 寄存器寻址。寄存器寻址是指指令所要的操作数已存储在某寄存器中，或把目标操作数存入寄存器。

(3) 直接寻址。直接寻址是指指令所要的操作数存放在内存中，在指令中直接给出该操作数的有效地址。

(4) 寄存器间接寻址。寄存器间接寻址是指操作数在存储器中，操作数的有效地址用 SI、DI、BX、BP 这 4 个寄存器之一来指定。

(5) 寄存器相对寻址。寄存器相对寻址是指操作数在存储器中，其有效地址是一个基址寄存器(BX、BP)或变址寄存器(SI、DI)的内容和指令中的 8 位/16 位偏移量之和。

(6) 基址加变址寻址。基址加变址寻址是指操作数在存储器中，其有效地址是一个基址寄存器(BX、BP)和一个变址寄存器(SI、DI)的内容之和。

(7) 相对基址加变址寻址。相对基址加变址寻址是指操作数在存储器中，其有效地址是一个基址寄存器(BX、BP)的值、一个变址寄存器(SI、DI)的值和指令中的 8 位/16 位偏移量之和。

3. 复杂指令集计算机

在计算机发展的早期，计算机技术水平较低，硬件较为简单，由硬件实现的指令系统的功能也就简单，一般只有定点的加减及逻辑运算、数据传送和程序转移等数十条最基本

的指令。随着计算机逻辑元件的迅猛发展，特别是超大规模集成电路的发展，机器的造价、体积、功耗及可靠性等方面都有了长足的发展；同时，随着计算机应用领域日益广泛，对指令系统功能的要求越来越高，使指令系统逐渐发展到几百种，寻址方式也更加灵活多样，具备这种指令系统的计算机称为复杂指令集计算机(Complex Instruction Set Computer，CISC)。

4. 精简指令集计算机

在指令系统中只有大约 20%的最简单的指令被经常使用，其使用频度达 80%。若只保留 20%的最简单的指令，使指令尽可能简单，从而设计一种硬件结构十分简单、执行速度很高的 CPU，这就是精简指令集计算机(RISC)。

13.1.1.7　系统可靠性基础

1. 基本概念

关于系统可靠性的基本概念如下。

(1) 系统的可靠性。系统的可靠性是指从系统开始运行(t=0)到某时刻 t 这段时间内能正常运行的概率，用 $R(t)$表示。

(2) 失效率。失效率是指单位时间内失效的元件数与元件总数的比例，通常用λ表示。当λ为常数时，可靠性与失效率的关系为 $R(t)=\mathrm{e}^{-\lambda t}$ 。

(3) 平均无故障时间(MTBF)。平均无故障时间是指两次故障之间系统能正常工作的时间的平均值。它与失效率的关系为 $\mathrm{MTBF}=1/\lambda$ 。

(4) 平均失效前时间(MTTF)。平均失效前时间是指从故障发生到机器修复平均所需要的时间。通常用平均修复时间(MTTR)来表示计算机的可维修性，即计算机的维修效率。

(5) 可用性。可用性是指计算机的使用效率，它以系统在执行任务的任意时刻能正常工作的概率 A 来表示，即 $A=\mathrm{MTBF}/(\mathrm{MTBF}+\mathrm{MTTR})$ 。

2. 系统可靠性模型

系统可靠性模型有以下几种。

(1) 串联系统。假设一个系统由 N 个子系统组成，当且仅当所有的子系统都能正常工作时，系统才能正常工作。

(2) 并联系统。假如一个系统由 N 个子系统组成，只要有一个子系统正常工作，系统就能正常工作。

(3) N 模冗余系统。由 N 个(N=2n+1)相同的逻辑线路和一个表决器组成，只要有 n+1 个或 n+1 个以上能正常工作，系统就能正常工作，输出正确的结果。

13.1.2　典型例题分析

例 13-1　在程序的执行过程中， Cache 与主存的地址映射是由__(1)__完成的。(2017 年下半年真题 1)

A. 操作系统　　B. 程序员调度

C. 硬件自动　　D. 用户软件

解析：Cache 地址的映射是由硬件实现的，以达到快速访问的目的，对用户和程序员是透明的。

答案：C

例 13-2 某四级指令流水线分别完成取指、取数、运算、保存结果四步操作。若完成上述操作的时间依次为 8ns、9ns、4ns、8ns，则该流水线的操作周期应至少为__(2)__ns。(2017 年下半年真题 2)

A. 4　　B. 8　　C. 9　　D. 33

解析：流水线的操作周期取决于基本操作时间最长的一个。

答案：C

例 13-3 内存按字节编址。若用存储容量为 32K×8bit 的存储器芯片构成地址从 A0000H 到 DFFFFH 的内存，则至少需要__(3)__片芯片。(2017 年下半年真题 3)

A. 4　　B. 8　　C. 16　　D. 32

解析：(DFFFFH−A0000H+1)/32K=8 片。

答案：B

例 13-4 计算机系统的主存主要是由__(4)__构成的。(2017 年下半年真题 4)

A. DRAM　　B. SRAM　　C. Cache　　D. EEPROM

解析：DRAM(动态随机存取存储器)需刷新，速度低，成本也低，是最为常见的系统内存。SRAM 无须刷新，功耗小，速度快，但集成度低，通常用于 CPU 和主存之间的高速缓存。

答案：A

例 13-5 计算机运行过程中，CPU 需要与外设进行数据交换。采用__(5)__控制技术时，CPU 与外设可并行工作。(2017 年下半年真题 5)

A. 程序查询方式和中断方式　　B. 中断方式和 DMA 方式

C. 程序查询方式和 DMA 方式　　D. 程序查询方式、中断方式和 DMA 方式

解析：程序查询方式中，CPU 通过执行程序查询外设的状态，判断外设是否准备好进行数据传送，由 CPU 全程控制，因此不能实现与外设的并行工作。DMA(直接存储器存取)采用专门的控制器来控制内存和外设之间的数据交流，无须 CPU 介入，大大提高了 CPU 的工作效率。中断方式在外设做好数据传送之前，CPU 可以做自己的事情，发出中断请求以后，CPU 响应才会控制其数据传输过程，一定程度上能实现 CPU 和外设的并行。

答案：B

例 13-6 CPU 执行算术运算或者逻辑运算时，常将源操作数和结果暂存在__(1)__中。(2017 年上半年真题 1)

A. 程序计数器(PC)　　B. 累加器(AC)

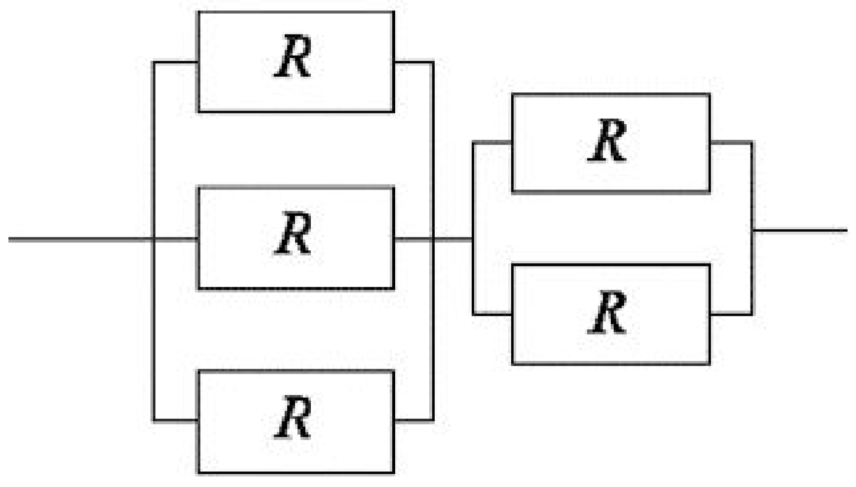
C. 指令寄存器(IR)　　D. 地址寄存器(AR)

解析：累加寄存器(AC)简称为累加器，其功能是：当运算器的算数逻辑单元(ALU)执行算术或逻辑运算时，为 ALU 提供一个工作区。累加寄存器暂存 ALU 运算中的结果信息。

答案：B

例 13-7 某系统由下图所示的冗余部件构成。若每个部件的千小时可靠度都为 R，则

该系统的千小时可靠度为__(2)__。(2017 年上半年真题 2)



A. $(1-R^3)(1-R^2)$　　B. $(1-(1-R)^3)(1-(1-R)^2)$

C. $(1-R^3)+(1-R^2)$　　D. $(1-(1-R)^3)+(1-(1-R)^2)$

解析：一个并联可靠度为：$1-(1-R)^3$，二个并联可靠度为：$1-(1-R)^2$，所以该系统串联的可靠度为$(1-(1-R)^3)(1-(1-R)^2)$。

答案：B

例 13-8　在程序运行过程中，CPU 需要将指令从内存中取出并加以分析和执行。CPU 依据__(1)__来区分在内存中以二进制编码形式存放的指令和数据。(2016 年下半年真题 1)

A. 指令周期的不同阶段　　B. 指令和数据的寻址方式

C. 指令操作码的译码结果　　D. 指令和数据所在的存储单元

解析：冯•诺依曼体系的计算机中指令和数据均以二进制的形式存放在存储器中，CPU 区分它们的方式是依据指令周期的不同阶段。

答案：A

例 13-9　常用的虚拟存储器由__(1)__两级存储器组成。(2013 年下半年真题 1)

A. 主存−辅存　　B. 主存−网盘　　C. Cache−主存　　D. Cache−硬盘

解析：本题考查的是虚拟内存方面的内容。

虚拟内存是计算机系统内存管理的一种技术。它使得应用程序认为它拥有连续的可用的内存(一个连续完整的地址空间)，而实际上，它通常是被分隔成多个物理内存碎片，还有部分暂时存储在外部磁盘存储器上，在需要时进行数据交换。所以虚拟存储器由主存−辅存(外存)两级存储器组成。

答案：A

例 13-10　计算机在一个指令周期的过程中，为从内存读取指令操作码，首先要将__(2)__中的内容送到地址总线上。(2016 年下半年真题 2)

A. 指令寄存器(IR)　　B. 通用寄存器(GR)

C. 程序计数器(PC)　　D. 状态寄存器(PSW)

解析：程序计数器(PC)用于存放下一指令的地址。计算机执行程序时，在一个指令周期中，要从内存读取指令操作码，首先需要将 PC 的内容送到地址总线上。

答案：C

例 13-11　设 16 位浮点数，其中阶符 1 位、阶码值 6 位，数符 1 位、尾数 8 位。若阶码用移码表示，尾数用补码表示，则该浮点数所能表示的数值范围是__(3)__。(2016 年下半年真题 3)

A. $-2^{64}\sim(1-2^{-8})\times2^{64}$　　B. $-2^{63}\sim(1-2^{-8})\times2^{63}$

C. $-(1-2^{-8})\times2^{64}\sim(1-2^{-8})\times2^{64}$　　D. $-(1-2^{-8})\times2^{63}\sim(1-2^{-8})\times2^{63}$

解析：浮点数的结构：尾数部分(定点小数)阶码部分(定点整数)。

9 位补码表示定点小数范围：$-1\sim+(1-2^{-8})$

也就是：$-1\sim+0.11111111$

非零最小正数：00…0,0.10…0；$(2^{-64})\,(2^{-1})$

最大正数：11…1,0.11…1；$(2^{63})(1-2^{-8})$

绝对值最小负数：00…0,1.011…1；$(2^{-64})[-(2^{-1}+2^{-8})]$

绝对值最大负数：11…1，1. 00…0；$(2^{63})(-1)$

故该浮点数能表示的数值范围是：$-2^{63}\sim(1-2^{-8})\times2^{63}$

答案：B

例 13-12　已知数据信息为 16 位，最少应附加__(4)__位校验位，以实现海明码纠错。(2016 年下半年真题 4)

A. 3　　B. 4　　C. 5　　D. 6

解析：海明码是利用奇偶性来检错和校验的方法，其构成方法是在数据位之间插入 r 个校验位来扩大码距从而实现纠错。N 表示添加了校验码位后整个传输信息的二进制位数，用 K 代表其中有效信息位数，r 表示添加的校验码位数，它们之间的关系应满足：$N=K+r\leqslant 2^r-1$。题中有效信息位为 16，计算得出最小应添加 5 位校验位。

答案：C

例 13-13　将一条指令的执行过程分解为取指、分析和执行 3 步，按照流水方式执行，若取指时间 $t_{取指}=4\Delta t$，分析时间 $t_{分析}=2\Delta t$，执行时间 $t_{执行}=3\Delta t$，则执行完 100 条指令，需要的时间为__(5)__Δt。(2016 年下半年真题 5)

A. 200　　B. 300　　C. 400　　D. 405

解析：流水线技术执行过程中，前后连续的几个操作可以依次进入，在这个站间重叠执行。执行完 100 条指令的时间为：$(4+2+3)\Delta t+(100-1)\times 4\Delta t=405\Delta t$。

答案：D

例 13-14　内存按字节编址，从 A1000H 到 B13FFH 的区域的存储容量为__(1)__KB。(2016 年上半年真题 1)

A. 32　　B. 34　　C. 65　　D. 67

解析：从 A1000H 到 B13FFH 的存储单元数为(B13FFH−A1000H)+1=10400H，存储容量为 10400H/1024=65KB。

答案：C

例 13-15　以下关于总线的叙述中，不正确的是__(2)__。(2016 年上半年真题 2)

A. 并行总线适合近距离高速数据传输

B. 串行总线适合长距离数据传输

C. 单总线结构在一个总线上适应不同种类的设备，设计简单且性能很高

D. 专用总线在设计上可以与连接设备实现最佳匹配

解析：在单总线结构中，CPU 与主存之间、CPU 与 I/O 设备之间、I/O 设备与主存之间、各种设备之间都通过系统总线交换信息。单总线结构的优点是控制简单方便，扩充方便。但由于所有设备部件均挂在单一总线上，使这种结构只能分时工作，即同一时刻只能在两个设备之间传送数据，这就使系统总体数据传输的效率和速度受到限制，这是单总线结构的主要缺点。

答案：C

例 13-16 CPU 是在__(1)__结束时响应 DMA 请求的。(2015 年下半年真题 1)

A. 一条指令执行　B. 一段程序　C. 一个时钟周期　D. 一个总线周期

解析：外设向 DMA 控制器(DMAC)提出 DMA 传送的请求；然后 DMA 控制器向 CPU 提出请求；CPU 在完成当前的总线周期后立即对此请求作出响应。总线周期通常指的是 CPU 完成一次访问存储器或 I/O 端口操作所需要的时间。

答案：D

例 13-17 在机器指令的地址字段中，直接指出操作数本身的寻址方式称为__(3)__。(2015 年下半年真题 3)

A. 隐含寻址　B. 寄存器寻址　C. 立即寻址　D. 直接寻址

解析：隐含寻址：这种类型的指令，不是明显地给出操作数的地址，而是在指令中隐含着操作数的地址。

寄存器寻址：当操作数不放在内存中，而是放在 CPU 的通用寄存器中时，可采用寄存器寻址方式。显然，此时指令中给出的操作数地址不是内存的地址单元号，而是通用寄存器的编号。

立即寻址：指令的地址字段指出的不是操作数的地址，而是操作数本身。立即寻址方式的特点是指令执行时间很短，因为它不需要访问内存取数，从而节省了访问内存的时间。

直接寻址：是一种基本的寻址方法。其特点是：在指令格式的地址的字段中直接指出操作数在内存的地址。由于操作数的地址直接给出而不需要经过某种变换，因此称这种寻址方式为直接寻址方式。

答案：C

例 13-18 内存按字节编址从 B3000H 到 DABFFH 的区域其存储容量为__(4)__。(2015 年下半年真题 4)

A. 123KB　B. 159KB　C. 163KB　D. 194KB

解析：存储地址从 B3000H 到 DABFFH 共有 DABFFH−B3000H+1=27C00H=159KB 个存储单元，由于内存地址按字节编址，所以存储容量为 159KB。

答案：B

例 13-19 某机器字长为 n 位的二进制数可以用补码来表示__(1)__个有符号定点小数。(2015 年上半年真题 1)

A. 2^n　B. 2^n-1　C. 2^{n-1}　D. $2^{n-1}+1$

解析：机器字长为 n 位时，补码可表示的定点小数范围为 $-1\sim+(1-2^{-(n-1)})$，一共有 2^n 个数。

答案：A

例 13-20 计算机中 CPU 对其访问速度最快的是__(2)__。(2015 年上半年真题 2)

A. 内存　B. Cache　C. 通用寄存器　D. 硬盘

解析：题目中 4 种存储设备按访问速度排序为：通用寄存器> Cache>内存>硬盘。

答案：C

例 13-21 计算机中 CPU 的中断响应时间指的是__(3)__的时间。(2015 年上半年真题 3)

A. 从发出中断请求到中断处理结束　B. 从中断处理开始到中断处理结束

C. CPU 分析判断中断请求　　　　　　D. 从发出中断请求到开始进入中断处理程序

解析：中断响应时间是指计算机接收到中断信号到操作系统作出响应，并完成切换转入中断服务程序的时间。广义上的中断响应时间是指，从来自 CPU 内部或外部的中断信号发生的时刻，到 CPU 完成当前现场保存，而进入此中断信号对应的处理程序的入口处的时刻，所经历的时间。

答案：D

例 13-22　以下关于指令流水线性能度量的叙述中，错误的是__(5)__。(2015 年上半年真题 5)

A. 最大吞吐率取决于流水线中最慢一段所需的时间

B. 流水线出现断流，加速比会明显下降

C. 要使加速比和效率最大化应该对流水线各级采用相同的运行时间

D. 流水线采用异步控制会明显提高其性能

解析：流水线若采用异步控制方式，流水线输出端任务流出的顺序与输入端任务流入的顺序可以不同，允许后进入流水线的任务先完成，会导致执行顺序混乱，影响程序的执行效率。

答案：D

13.1.3　同步练习

1. 属于 CPU 中算术逻辑单元的部件是________。

A. 程序计数器　　B. 加法器　　C. 指令寄存器　　D. 指令译码器

2. 内存按字节编址从 A5000H 到 DCFFFH 的区域其存储容量为________。

A. 123KB　　B. 180KB　　C. 223KB　　D. 224KB

3. 计算机采用分级存储体系的主要目的是解决________的问题。

A. 主存容量不足　　B. 存储器读写可靠性

C. 外设访问效率　　D. 存储容量、成本和速度之间的矛盾

4. 在 CPU 中，常用来为 ALU 执行算术逻辑运算提供数据并暂存运算结果的寄存器是________。

A. 程序计数器　　B. 状态寄存器　　C. 通用寄存器　　D. 累加寄存器

5. 某机器字长为 n，最高位是符号位，其定点整数的最大值为________。

A. 2^n-1　　B. $2^{n-1}-1$　　C. 2^n　　D. 2^{n-1}

6. 通常可以将计算机系统中执行一条指令的过程分为取指令、分析指令和执行指令 3 步。若取指令时间为 $4\Delta t$，分析指令时间为 $2\Delta t$，执行指令时间为 $3\Delta t$，按顺序方式从头到尾执行完 600 条指令所需时间为__(1)__Δt；若按照执行第 i 条、分析第 $i+1$ 条、读取第 $i+2$ 条重叠的流水线方式执行指令，则从头到尾执行完 600 条指令所需时间为__(2)__Δt。

(1) A. 2400　　B. 3000　　C. 3600　　D. 5400

(2) A. 2400　　B. 2405　　C. 3000　　D. 3009

7. 若用 256K×8bit 的存储器芯片，构成地址 40000000H 到 400FFFFFH 且按字节编址的内存区域，则需________片芯片。

A.4　　B.8　　C.16　　D.32

13.1.4　同步练习参考答案

1. B　　2. D　　3. D　　4. D　　5. B
6. (1) D　(2) B　　7. A

13.2　操 作 系 统

13.2.1　考点辅导

13.2.1.1　操作系统的基本概念

操作系统(Operating System，OS)是计算机系统中的一个系统软件，它能有效地组织和管理系统中的各种硬件和软件资源，合理地组织计算机系统工作流程，控制程序的执行，并向用户提供一个良好的工作环境和友好的接口。

操作系统主要有并发性(Concurrency)、共享性(Sharing)、虚拟性(Virtual)和不确定性(Non-Determinacy) 4 个基本特征。

1. 操作系统的功能

操作系统具有如下功能。

(1) 进程管理：包括进程控制、进程通信和进程调度。

(2) 存储管理：包括存储分配和回收、存储保护、地址映射和主存扩充。

(3) 设备管理：包括对输入输出设备的分配、启动、完成和回收。

(4) 文件管理：包括文件存储空间管理、目录管理、文件的读写管理和存取控制。

(5) 作业管理：包括任务、界面管理、人机交互、图形界面、语音控制和虚拟现实等。

2. 操作系统的分类

根据操作系统的使用环境和对作业的处理方式来划分，操作系统的基本类型有批处理操作系统、分时系统、实时系统、网络操作系统、分布式操作系统、微机操作系统、嵌入式操作系统。

13.2.1.2　处理机管理

1. 进程的基本概念

进程是一个程序在一个数据集合上的一次执行，是操作系统中可以并行工作的基本单位，也是核心调度及资源分配的最小单位。它由程序、数据、进程控制块(PCB)组成。进程与程序的重要区别之一是：进程是有状态的；而程序没有，程序是静态的。

进程的基本特征有动态性、并发性、独立性、异步性、结构性。

传统上，每个进程在任何时刻总是处于 3 种基本状态(即运行、就绪、阻塞)的某一种基本状态。在不少系统中，还增加了两种基本状态，即新建态、终止态。状态之间的转换如图 13-2 所示。

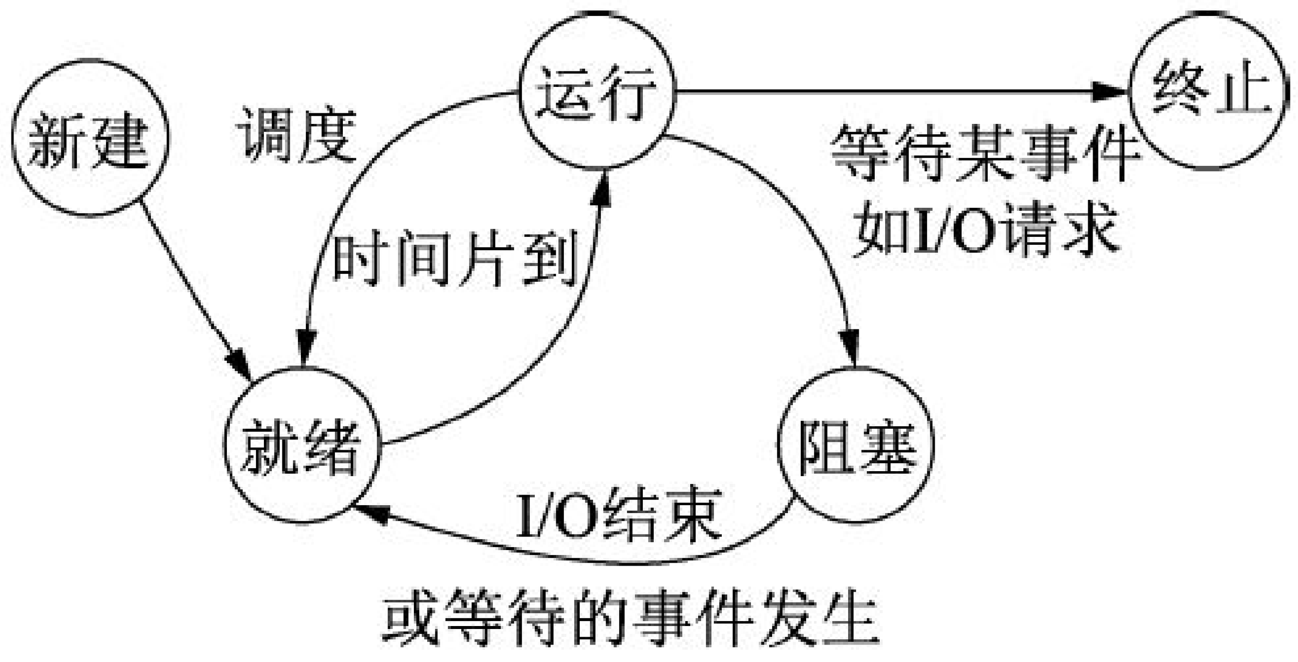


图 13-2 进程状态的转换

2. 线程

在 SMP 系统中，操作系统还提供了线程机制。线程是比进程更小的能独立运行的基本单位，它是处理器分配的最小单位。

进程是资源分配的基本单位，而线程与资源分配无关，它属于某一个进程，并与进程内的其他线程一起共享进程的资源。线程也有就绪、阻塞和运行 3 种基本状态。

3. 进程间通信

1) 同步与互斥

(1) 进程间的同步。一个进程相对于另一个进程的运行速度是不确定的，也就是说，进程是在异步环境下运行的。每个进程都以各自独立的、不可预知的速度向前推进。但相互合作的进程需要在某些确定点上协调它们的工作，当一个进程到达了这些点后，除非另一进程已经完成了某些操作；否则就不得不停下来等待这些操作结束。

(2) 进程间的互斥。在多道程序系统中，各进程可以共享各类资源，但有些资源一次只能供一个进程使用，称为临界资源(Critical Resource，CR)，如打印机、公共变量和表格等。同步是进程间的直接制约问题，互斥是进程间的间接制约问题。

2) 信号量机制

信号量是一种解决进程同步与互斥的工具。主要有整型信号量、记录型信号量、信号量集机制。最常用的信号量是整型变量。

信号量可分为两类：一类是公用信号量，用于实现进程间的互斥，初值等于 1 或资源的数目；另一类是私用信号量，用于实现进程间的同步，初值等于 0 或某个正整数。信号量 S 的物理意义是：当 $S\geqslant 0$ 时，表示某资源的可用数；当 $S<0$ 时，其绝对值表示阻塞队列中等待该资源的进程数。

3) PV 操作

PV 操作是实现进程同步与互斥的常用方法。PV 操作是低级通信原语，在执行期间不可分割。其中，P 操作表示申请一个资源，V 操作表示释放一个资源。

P 操作定义：$S:=S-1$，若 $S\geqslant 0$，则执行 P 操作的进程继续执行；否则，若 $S<0$，则置该进程为阻塞状态(因为无可用资源)，并将其插入阻塞队列。

V 操作定义：$S:=S+1$，若 $S>0$，则执行 V 操作的进程继续执行；否则，若 $S\leqslant 0$，则从阻塞状态唤醒一个进程，并将其插入就绪队列，执行 V 操作的进程继续执行。

利用 PV 操作实现进程互斥的方法为：令信号量 mutex 的初值为 1，当进程进入临界区时执行 P 操作，退出临界区时执行 V 操作。

利用 PV 操作实现进程同步的方法为：用一个信号量与消息联系起来。当信号量的值为“0”时表示希望的消息未产生，当信号量的值为非“0”时表示希望的消息已经存在。假定用信号量 S 表示某条消息，进程可以通过调用 P 操作测试消息是否到达，调用 V 操作通知消息已准备好。最典型的就是单缓冲区的生产者和消费者的同步问题。

4. 进程调度算法

进程调度算法有以下几种。

(1) 先来先服务调度算法：按进程进入就绪队列的先后次序选择可以占用处理器的进程。

(2) 优先数调度算法：对每个进程确定一个优先数，进程调度总是让具有最高优先数的进程先使用处理器。如果进程具有相同的优先数，则对这些有相同优先数的进程再按先来先服务的次序分配处理器。

(3) 时间片轮转调度算法：把规定进程一次使用处理器的最长时间称为“时间片”。让就绪进程按就绪的先后次序排成队列，每次总是选择就绪队列中的第一个进程占用处理器，但规定只能使用一个“时间片”。如果一个时间片用完，进程工作尚未结束，则它也必须让出处理器给其他进程使用，自己被重新排到就绪队列的末尾，等待再次运行。时间片轮转调度算法经常用在分时操作系统中。

(4) 分级调度算法：由系统设置多个就绪队列，每个就绪队列中的进程按时间片轮转调度算法占用处理器。

5. 死锁

1) 产生死锁的原因

若系统中存在一组进程，它们中的每个进程都占用了某种资源，而又都在等待其中另一个进程所占用的资源，这种等待永远不能结束，则说明系统出现了死锁。只要下面 4 个条件中有 1 个不具备，系统就不会出现死锁。

(1) 互斥条件：某个资源在一段时间内只能由一个进程占有，不能同时被两个或两个以上的进程占有。

(2) 不可抢占条件：进程所获得的资源在未使用完毕之前，资源申请者不能强行地从资源占有者手中夺取资源，而只能由该资源的占有者进程自行释放。

(3) 占有且申请条件：进程至少已经占有一个资源，但又申请新的资源；由于该资源已被另外进程占有，此时该进程阻塞；但是，它在等待新资源时，仍继续占用已占有的资源。(注：也称为保持与等待条件)

(4) 循环等待条件：存在一组进程等待序列$\{P_1, P_2,\cdots,P_n\}$，其中 P_1 等待 P_2 所占有的某一资源，P_2 等待 P_3 所占有的某一资源，……，而 P_n 等待 P_1 所占有的某一资源，形成一个进程循环等待环。

2) 死锁的预防方法

死锁的预防方法如下。

(1) 打破互斥条件。

(2) 打破不可抢占条件。

(3) 打破占有且申请条件。

13.2.1.3　存储管理

1. 分页存储管理

1)　分页原理

将一个进程的地址空间划分成若干大小相等的区域，称为页。相应地，将主存空间划分成与页相同大小的若干物理块，称为块或页框架。在为进程分配主存时，将进程中若干页分别装入多个不邻接的块中。

2)　地址结构

地址由两部分组成：前一部分为页号 P；后一部分为偏移量 W，即页内地址。图 13-3 中的地址长度为 32 位，其中第 0～11 位为页内地址(每页的大小为 4KB)，第 12～31 位为页号，所以允许地址空间的大小最多为 1MB 个页。

31　　　　　　　　12	11　　　　　　0
页号P	页内地址W

图 13-3　分页地址结构

3)　地址变换

系统为每个进程建立了一张页面映射表，简称页表。每个页在页表中占一个表项，记录该页在内存中对应的物理块号。进程在执行时，通过查找页表，就可以找到每页所对应的物理块号。可见，页表的作用是实现从页号到物理块号的地址映射。

2. 分段存储管理

1)　分段基本原理

作业的地址空间被划分为若干段，每个段定义了一组逻辑信息。每个段都有自己的名字，都是从零开始编址的一段连续的地址空间。段的长度由相应逻辑信息组的长度决定，因而各段长度不等。整个作业的地址空间是二维的。分段系统中地址结构如图 13-4 所示，其逻辑地址由段号(名)和段内地址两部分组成，在该地址结构中，允许一个作业最多能有 256 个段，每个段的最大长度为 64KB。

23　　　　18	17　　　　　　　　0
段号S	段内地址W

图 13-4　分段地址结构

2)　地址变换机构

在分段式存储管理系统中，为每个段分配一个连续的分区，而进程中的各个段可以离散地分配到内存中不同的分区中。在系统中为每个进程建立一张段映射表，简称为“段表”。进程在执行中，通过查段表来找到每个段所对应的内存区。所以说，段表实现了从逻辑段到物理内存区的映射。

3. 虚拟存储管理

1)　局部性原理

局部性原理是虚拟存储技术的理论基础，是指程序的执行往往呈现出高度的局限性，即程序执行时往往会不均匀地访问内存储器。程序的局限性表现为以下特征。

(1) 时间局部性：若一条指令被执行，则在不久的将来，它可能再被执行。

(2) 空间局部性：一旦一个存储单元被访问，则它附近的单元也将很快被访问。

2) 虚拟存储器的定义

利用大容量的外存(通常是高速硬盘)来扩充内存，产生一个比有限的实际内存空间大得多的、逻辑的虚拟内存空间，以便能够有效地支持多道程序系统的实现和大型作业运行的需要，从而增强系统的处理能力。当进程要求运行时，不是将它的全部信息装入内存，而是将其一部分先装入内存，另一部分暂时留在外存。进程在运行过程中，要使用的信息不在内存时，发生中断，由操作系统将它们调入内存，以保证进程的正常运行。从用户角度看，该系统所具有的主存容量，将比实际主存容量大得多，人们把这样的存储器称为虚拟存储器。

3) 虚拟存储器的实现

虚拟存储器的实现方法如下。

(1) 请求分页系统。在分页系统的基础上，增加了请求调页功能和页面置换功能所形成的页式虚拟存储系统。请求分页机制是在纯分页的页表机制上形成的，由于只将应用程序的一部分调入主存，还有一部分仍在磁盘上，故需在页表中再增加若干项，如状态位、访问字段、辅存地址等供程序(数据)在换进、换出时引用。在请求分页系统中，每当所要访问的页面不在主存时，便要产生一个缺页中断，请求操作系统将所缺页调入主存。它与一般中断的主要区别在于：缺页中断在指令执行期间产生和处理中断信号，而一般中断在一条指令执行完后检查和处理中断信号；缺页中断返回到该指令的开始重新执行该指令，而一般中断返回到该指令的下一条指令执行。

(2) 请求分段系统。在分段系统的基础上，增加了请求调段和分段置换功能所形成的段式虚拟存储系统。

4) 替换算法

替换算法有以下几种。

(1) 最佳置换(OPT)算法。OPT 算法是一种理论化的算法。该算法淘汰在访问串中将来再也不出现的或是在最长时间内不再访问的页。这样，被淘汰掉的页将不会造成因需要访问该页又需要把它调入的现象。这种最佳策略本身不是一种实际的方法，它的理论价值在于：用 OPT 算法的缺页率去评价其他算法的优劣。

(2) 先进先出(FIFO)算法。FIFO 算法总是选择作业中在主存驻留时间最长(即最老)的一页淘汰，即先进入主存的页先退出主存。其理由是，最早调入主存的页，其不再被使用的可能性比最近调入主存的页要大。

(3) 最近最久未使用置换(LRU)算法。LRU 算法选择在最近一段时间内最久不用的页予以淘汰。这是最常用的页面置换算法。

(4) 最近未用置换(NUR)算法。NUR 算法是将最近一段时间未引用过的页面换出。它是一种 LRU 的近似算法。

13.2.1.4 设备管理

1. DMA 技术与缓冲技术

1) DMA 技术

DMA(Directed Memory Access)的基本思想是：在外围设备和主存之间开辟直接的数据

交换通路；在内存与输入输出设备间传送一个数据块的过程中，不需要 CPU 的任何干涉，只需要 CPU 在过程开始启动与过程结束时的处理，实际操作由 DMA 硬件直接执行完成。

2) 缓冲技术

引入缓冲技术的目的是：缓和 CPU 和 I/O 设备间速度不匹配的矛盾；提高它们之间的并行性；减少对 CPU 的中断次数，放宽 CPU 对中断响应时间的要求。

缓冲技术可以采用硬件缓冲和软件缓冲两种。硬件缓冲是利用专门的硬件寄存器作为缓冲区；软件缓冲是利用操作系统的管理，用主存中的一个或多个区域作为缓冲区，进而可以形成缓冲池。

2. Spooling 系统

1) Spooling 技术

Spooling 技术是用一类物理设备模拟另一类物理设备的技术，可以将低速的独占设备改造成一种可共享的设备，而且一台物理设备可以对应若干台虚拟的同类设备。Spooling 技术的引入缓和了 CPU 与设备速度的不均匀性问题，提高了 CPU 与设备的并行程度。

2) Spooling 系统的组成

Spooling 系统由“预输入程序”“缓输出程序”和“井管理程序”以及输入和输出井组成，如图 13-5 所示。

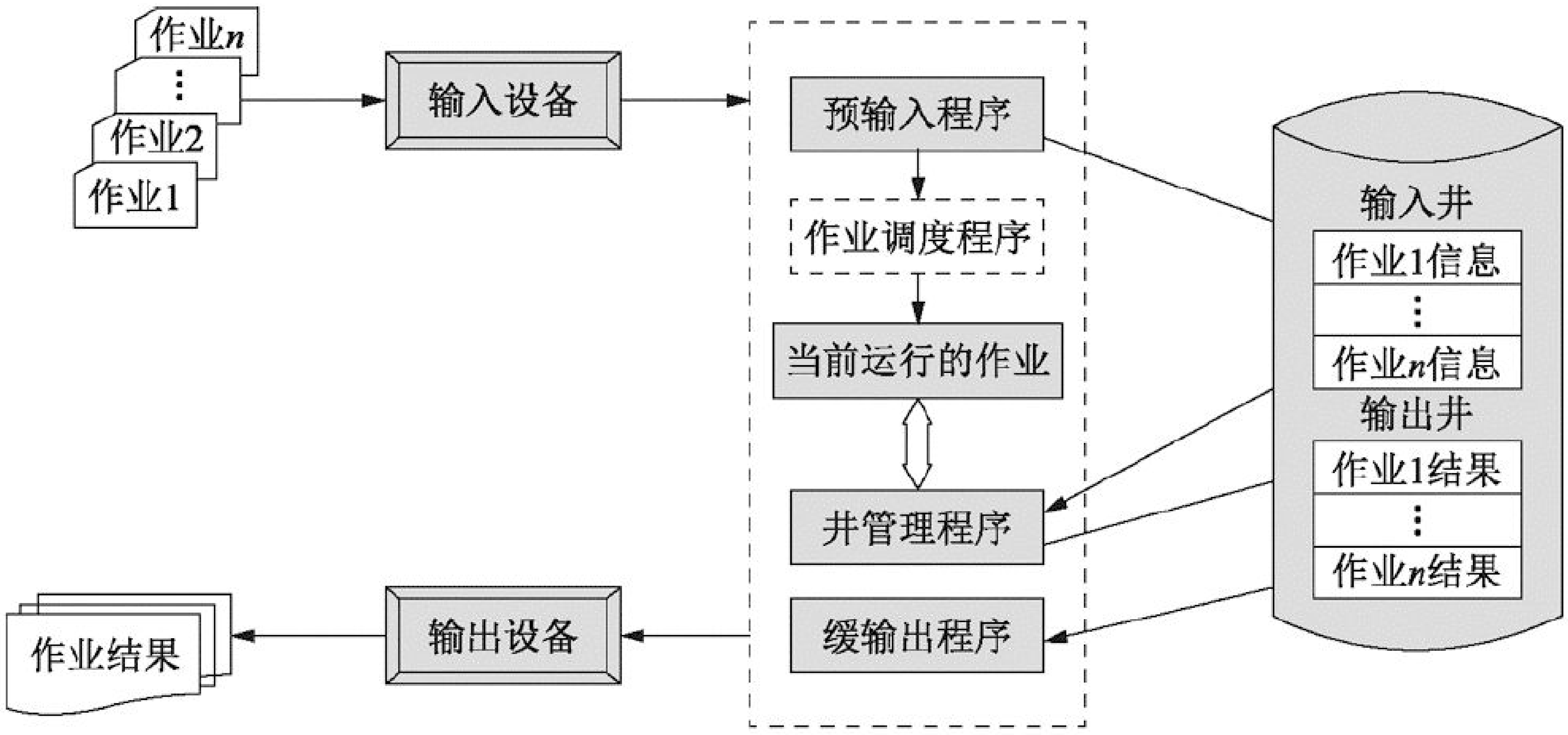


图 13-5　Spooling 系统的组成

3) Spooling 系统的工作过程

Spooling 系统将一个作业从进入系统到完成后撤离系统的全过程，划分成输入、处理和输出 3 个并发执行的过程。当用户作业要进入系统时，由 Spooling 系统的预输入程序将作业信息从物理输入设备上送到磁盘上指定区域(称为输入井)。输入井中的作业有 4 种状态。

(1) 输入状态：作业的信息正从输入设备上预输入。

(2) 收容状态：作业预输入结束但未被选中执行。

(3) 执行状态：作业已被选中进入运行过程中，它可从输入井中读取数据信息，也可向输出井写信息。

(4) 完成状态：作业已经撤离，该作业的执行结果等待缓输出。

13.2.1.5　文件管理

文件是信息的一种组织形式，是存储在辅助存储器上的具有标识名的一组集合。操作系统中由文件系统来管理文件的存储、检索、更新、共享和保护。文件系统包括两方面：一方面是负责管理文件的一组系统软件，另一方面是文件本身。

1. 文件的类型

根据文件的性质和用途，文件有多种分类方法。

(1) 按文件的用途，可以分为系统文件、库文件和用户文件等。

(2) 按信息保存期限，分为临时文件、档案文件和永久文件。

(3) UNIX 系统将文件分为普通文件、目录文件和设备文件(特殊文件)等。

(4) 按文件的保护方式，可分为只读文件、读写文件、可执行文件和不保护文件等。

目前常用的文件系统类型有 FAT、VFAT、NTFS、Ext2、HPFS 等。

2. 文件的结构

文件的结构是指文件的组织形式。从用户观点所看到的文件组织形式，称为文件的逻辑结构；从实现观点考察文件在辅助存储器上的存放方式，常称为文件的物理结构。

1) 逻辑结构

逻辑结构分为两种，即无结构的字符流文件和有结构的记录文件。记录文件由记录组成，即文件内的信息划分成多个记录，以记录为单位组织和使用信息。记录文件有顺序文件、索引顺序文件、索引文件和直接文件。

2) 物理结构

物理结构是文件在存储设备上的存放方法。物理块是分配和传输信息的基本单位。常用的文件物理结构有连续结构、链接结构、索引结构。

3. 文件目录

文件目录是文件控制块的集合。通常文件目录也被组织成文件，称为目录文件。文件系统一般采用一级目录结构、二级目录结构和多级目录结构。DOS、UNIX、WIN 都是采用多级目录结构。

工作目录也称当前目录。在多级目录结构的文件系统中，文件的全路径名可能较长，也会涉及多次磁盘访问，为了提高效率，操作系统提供设置工作目录的机制。每个用户都有自己的工作目录。任一目录节点都可以被设置为工作目录。一旦某个目录节点被设置成工作目录，相应的目录文件有关内容就会被调入主存，这样，对以工作目录为根的子树内任一文件的查找时间会缩短。从工作目录出发的文件路径名称为文件的相对路径名。文件系统允许用户随时改变自己的工作目录。

4. 文件的存取方法和存取控制

1) 文件的存取方法

文件的存取方法是指读、写文件存储器上的一个物理块的方法。通常有顺序存取、随机存取和按键存取等。

2) 文件存储空间的管理

文件存储空间的管理实质是对空闲块的组织和管理问题。它包括空闲块的组织、分配和回收等。常用的文件存储空间的管理方法有位示图、空闲块表和空闲块链 3 种。

5. 文件的使用

一般文件系统提供一组专门用于文件、目录的管理的命令，如目录管理、文件控制和文件存取等命令。

(1) 目录管理命令，如建立目录、显示工作目录、改变目录、删除目录(一般只可删除空目录)。

(2) 文件控制命令，如建立文件、删除文件、打开文件、关闭文件、改文件名、改变文件属性。

(3) 文件存取命令，如读/写文件、显示文件内容、复制文件等。

6. 文件的共享和保护

文件共享是指不同的用户使用同一文件。文件的共享可以采用文件的绝对路径名(或相对路径名)共享同一文件。

文件保护是指避免文件拥有者或其他用户有意或无意地使文件受到破坏。这两个问题涉及用户对文件进行访问的权限，即文件的访问控制。常见的文件访问控制方式有访问控制矩阵、访问控制表、用户权限表、口令和密码。

文件的安全是指文件的保密和保护，即限制未授权用户使用或破坏文件。常常在系统级、用户级、目录级和文件级上实施。对目录和文件的访问权限可以由建立者设置。除了限定访问权限，还可以通过加密等方式进行保护。

13.2.1.6 作业管理

作业是用户在一次上机过程中，要求计算机所做的工作的集合。作业由程序、数据和作业说明书 3 部分组成。其中，作业说明书包括作业基本情况、作业控制、作业资源要求的描述，它体现用户的控制意图。

作业控制块(JCB)是记录该作业的有关信息。JCB 是作业存在的唯一标志，主要包括作业名、作业状态、资源要求、作业控制方式、作业类型及作业优先级。

1. 作业的状态

作业的状态分为 4 种：提交、后备、执行和完成，它们之间的转换如图 13-6 所示。

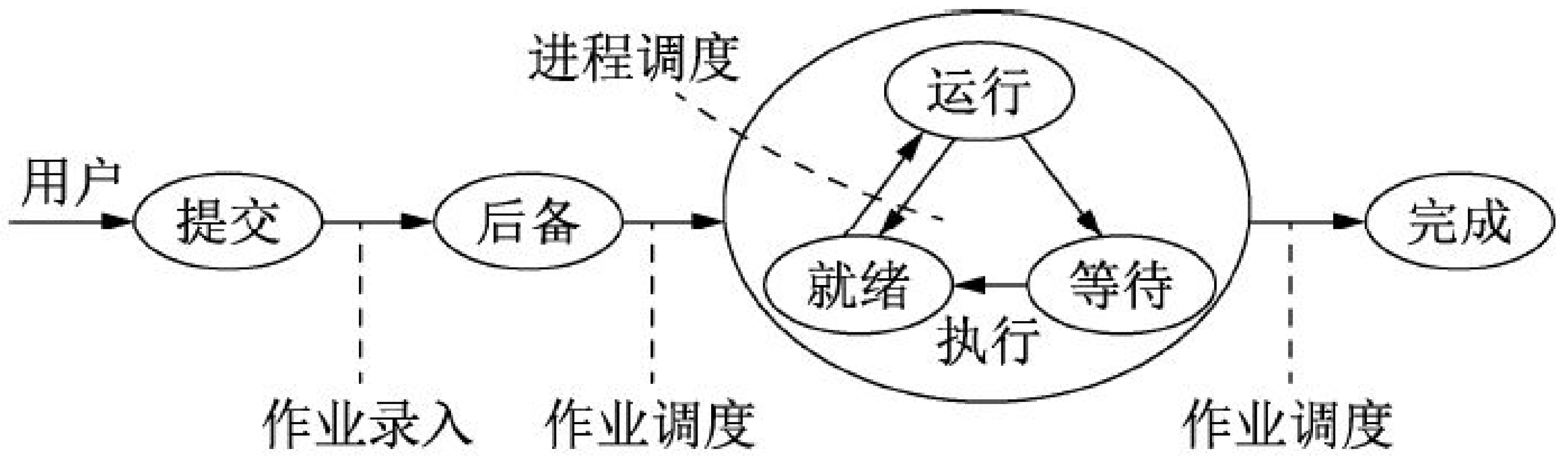


图 13-6 作业调度与进程调度

2. 作业调度算法

作业调度算法有以下几种。

(1) 先来先服务(FCFS)算法：最简单的算法，它按照作业到达先后次序来挑选作业，先进入的作业优先被挑选。

(2) 最短作业优先(SJF) 算法：作业的长短是以要求运行的时间来衡量的。最短作业优先算法总是优先调度要求运行时间最短的作业，把它作为下一次服务的对象。

(3) 响应比高优先(HRN)算法：响应比高的作业优先启动。定义响应比为

$$R_{\mathrm{p}}=\frac{\text{作业响应时间}}{\text{作业执行时间}}$$

其中，作业响应时间为作业进入系统后的等候时间与作业的执行时间之和，因此，有

$$R_{\mathrm{p}}=1+\frac{\text{作业等待时间}}{\text{作业执行时间}}$$

(4) 优先级调度算法：为每个作业确定一个优先数，资源能满足且优先数高的作业优先被选取；当几个作业有相同优先数时，对这些具有相同优先数的作业再运用先来先服务算法进行调度。

(5) 均衡调度算法：根据作业对资源的要求进行分类，从各类作业中去挑选，尽可能地使得使用不同资源的作业同时被执行。

13.2.2　典型例题分析

例 13-23　某计算机系统页面大小为 4KB，进程的页面变换表如下所示。若进程的逻辑地址为 2D16H。该地址经过变换后，其物理地址应为__(8)__。(2017 年上半年真题 8)

页　号	物理块号
0	1
1	3
2	4
3	6

A. 2048H　　B. 4096H　　C. 4D16H　　D. 6D16H

解析：页面大小为 4KB=2^{12}B。逻辑地址 2D16H=0010110100010110=页号(2)+页内偏移量(即 D16)。根据页面变化表可知页号 2 对应物理块号 4，则其物理地址=物理块号(4)+偏移量(D16)，即 4D16。

答案：C

例 13-24　假设系统有 n 个进程共享资源 R，且资源 R 的可用数为 3，其中 $n\geqslant 3$，若采用 PV 操作，则信号量 S 的取值范围应为__(9)__。(2016 年下半年真题 9)

A. $-1\sim n-1$　　B. $-3\sim 3$　　C. $-(n-3)\sim 3$　　D. $-(n-1)\sim 1$

解析：资源 R 的可用数为 3，则信号量的初始值为 3，负数表示所缺资源数，共有 n 个进程，所缺资源数最多为 $n-3$(亦可理解为等待的进程数)，故信号量 S 的取值范围为：$-(n-3)\sim 3$。

答案：C

例 13-25　在 Windows 系统中，设 E 盘的根目录下存在 document1 文件夹，用户在该

文件夹下已创建了 document2 文件夹，而当前文件夹为 document1。若用户将 test.docx 文件存放在 document2 文件夹中，则该文件的绝对路径为 (8) ；在程序中能正确访问该文件且效率较高的方式为 (9) 。(2015 年下半年真题 8、9)

(8) A. \document1\　　B. E:\document1\ document2
C. document2\　　D. E:\document2\ document1

(9) A. \document1\test.docx　　B. document1\ document2\test.docx
C. document2\test.docx　　D. E:\document1\ document2\test.docx

解析：绝对路径是指从根目录开始的路径，也称为完全路径；相对路径是指从用户工作目录开始的路径。绝对路径是确定不变的，而相对路径则随着用户工作目录的变化而不断变化。显然，采用相对路径时访问效率较高。

答案：(8) B　(9) C

例 13-26　C 程序中全局变量的存储空间在 (7) 分配。(2015 年上半年真题 7)

A. 代码区　　B. 静态数据区
C. 栈区　　D. 堆区

解析：

代码区：存放函数体的二进制代码。

栈区：由编译器自动分配释放，存放函数的参数值、局部变量的值等。

堆区：一般由程序员分配释放；若程序员不释放，程序结束时可能由操作系统回收。

静态数据区：内存在程序启动的时候才被分配，而且可能直到程序开始执行的时候才被初始化，所分配的内存在程序的整个运行期间都存在，如全局变量、static 变量等。

答案：B

例 13-27　某进程有 4 个页面，页号为 0～3，页面变换表及状态位、访问位和修改位的含义如下图所示。系统给该进程分配了 3 个存储块，当采用第二次机会页面替换算法时，若访问的页面 1 不在内存，这时应该淘汰的页号为 (8) 。(2015 年上半年真题 8)

页　号	帧　号	状态位	访问位	修改位
0	6	1	1	1
1	—	0	0	0
2	3	1	1	1
3	2	1	1	0

状态位含义 {=0 不在内存；=1 在内存}
访问位含义 {=0 未访问过；=1 访问过}
修改位含义 {=0 未修改过；=1 修改过}

A. 0　　B. 1　　C. 2　　D. 3

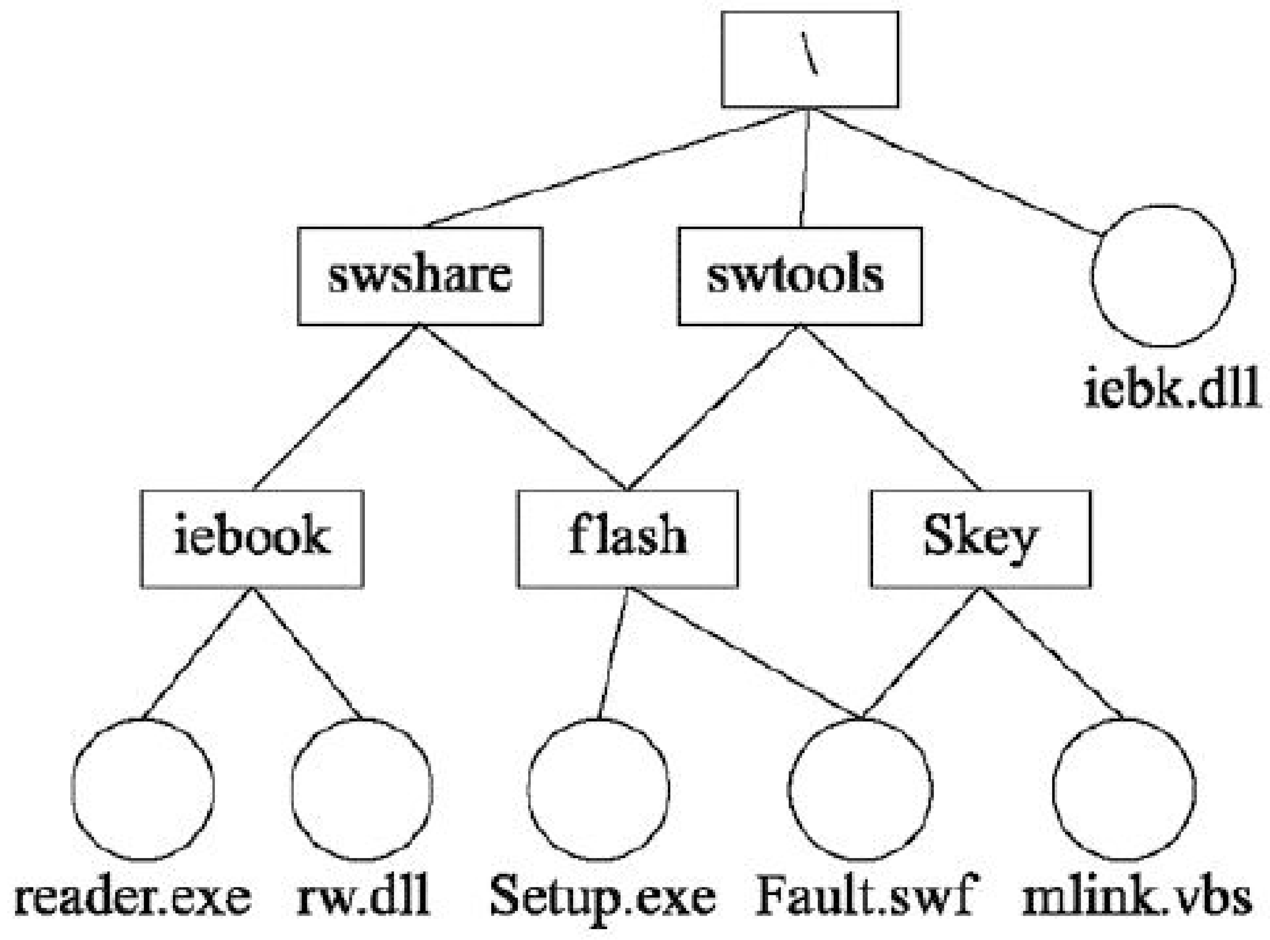
解析：页面 1 不在内存，可以直接排除选项 B。在本题中，内存中的 3 个页面，都是刚刚被访问过的。所以不能以访问位作为判断标准，只能看修改位。修改位中，只有 3 号页未被修改，如果淘汰 3 号页，直接淘汰即可，没有额外的工作要做；如果淘汰 0 号或 2 号，则需要把修改的内容进行更新，这样会有额外的开销。

答案：D

13.2.3　同步练习

1.　若某文件系统的目录结构如下图所示，假设用户要访问文件 fault.swf，且当前工作

目录为 swshare，则该文件的全文件名为__(1)__，相对路径和绝对路径分别为__(2)__。



(1) A. fault.swf　　B. flash\fault.swf
C. swshare\flash\fault.swf　　D. \swshare\flash\fault.swf

(2) A. swshare\flash\和\flash\　　B. flash\和\swshare\flash\
C. \swshare\flash\和 flash\　　D. \flash\和\swshare\flash\

2. 设系统中有 *R* 类资源 *m* 个，现有 *n* 个进程互斥使用。若每个进程对 *R* 资源的最大需求为 *w*，那么当 *m*、*n*、*w* 取下表的值时，对于下表中的 a～e 5 种情况，__(1)__两种情况可能会发生死锁。对于这两种情况，若将__(2)__，则不会发生死锁。

	a	b	c	d	e
m	2	2	2	4	4
n	1	2	2	3	3
w	2	1	2	2	3

(1) A. a 和 b　　B. b 和 c　　C. c 和 d　　D. c 和 e

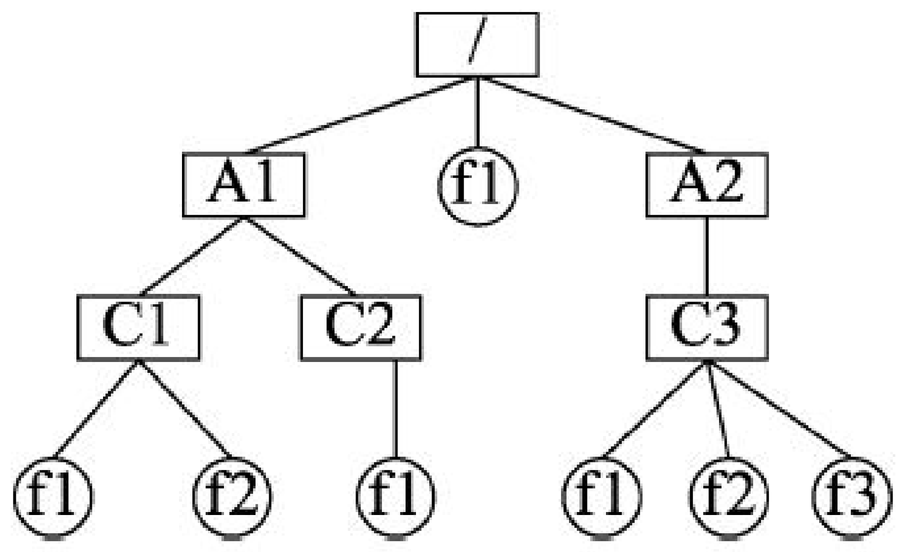
(2) A. *n* 加 1 或 *w* 加 1　　B. *m* 加 1 或 *w* 减 1
C. *m* 减 1 或 *w* 加 1　　D. *m* 减 1 或 *w* 减 1

3. 内存采用段式存储管理有许多优点，但______不是其优点。
A. 分段是信息逻辑单位，用户不可见　　B. 各段程序的修改互不影响
C. 地址变换速度快，内存碎片少　　D. 便于多道程序共享主存的某些段

4. 在下图所示的树型文件系统中，方框表示目录，圆圈表示文件，“/”表示路径中的分隔符，“/”在路径之首时表示根目录。图中，__(1)__。假设当前目录是 A2，若进程 A 以如下两种方式打开文件 f2：

方式①　　fd1=open(“__(2)__ /f2”,o_RDONLY);
方式②　　fd1=open(“/A2/C3/f2”,o_RDONLY);

那么，采用方式①的工作效率比方式②的工作效率高。



(1) A. 根目录中文件 f1 与子目录 C1、C2 和 C3 中文件 f1 相同
B. 子目录 C1 中文件 f2 与子目录 C3 中文件 f2 是相同的
C. 子目录 C1 中文件 f2 与子目录 C3 中文件 f2 是不同的
D. 子目录 C1 中文件 f2 与子目录 C3 中文件 f2 可能相同也可能不相同

(2) A. /A2/C3 B. /A2/C3 C. C3 D. f2

13.2.4 同步练习参考答案

1. (1) D (2) B 2. (1) D (2) B 3. C 4. (1) D (2) C

13.3 系统开发和运行基础

13.3.1 考点辅导

13.3.1.1 需求分析和设计方法

1. 软件工程

1) 软件工程的概念

为了消除软件危机，通过认真研究解决软件危机的方法，人们认识到软件工程是使计算机软件走向科学的途径，逐渐形成了软件工程的概念，并开辟工程学的新兴领域，即软件工程学。

2) 软件工程的要素

软件工程具有以下 3 个要素。

(1) 方法。完成软件工程项目的技术手段。

(1) 工具。支持软件的开发、管理、文档生成。

(3) 过程。将方法和工具综合起来以达到合理、及时地进行计算机软件开发的目的。

3) 软件生命周期

软件生命周期是指软件产品从考虑其概念开始到该软件产品交付使用，直至最终退役为止的整个过程，包括计划阶段、分析阶段、设计阶段、实现阶段、测试阶段和运行维护阶段。

4) 软件开发模型

比较经典的软件开发模型有瀑布模型、快速原型模型、演化模型、增量模型、螺旋模型、喷泉模型等。

5) 软件开发方法

软件开发方法有以下几种。

(1) 结构化软件开发(SASD)方法：采用结构化技术来完成软件开发的各项任务。它把软件生命周期划分成若干个阶段，依次完成每个阶段的任务。它与瀑布模型有很好的结合度，是与其最相适应的软件开发方法。

(2) 面向数据结构的软件开发方法：从目标系统的输入、输出数据结构入手，导出程

序框架结构，再补充其他细节，从而可得到完整的程序结构图。有 Jackson 方法和 Warnier 方法。

(3) 面向对象的软件开发方法：随着 OOP(面向对象编程)向 OOD(面向对象设计)和 OOA(面向对象分析)的发展，最终形成面向对象的软件开发方法 OMT(Object Modelling Technique)。这是一种自底向上和自顶向下相结合的方法，而且它以对象建模为基础，从而不仅考虑了输入、输出数据结构，实际上也包含了所有对象的数据结构。

(4) 基于构件化的开发方法：用预先建立的构件和模板，像“搭积木”一样进行建造。

2. 需求分析

需求分析包括以下内容。

(1) 任务：①确定软件系统的功能需求和非功能需求；②分析软件系统的数据要求；③导出系统的逻辑模型；④修正项目开发计划；⑤如有必要，可以开发一个原型。

(2) 主要工作：①需求获取——确定对目标系统的各方面需求。涉及的主要任务是建立获取用户需求的方法框架，并支持和监控需求获取的过程。②需求分析和综合——对问题进行分析，然后在此基础上整合出解决方案。③编写需求规格说明书——对已确定的需求进行文档化描述，该文档通常称为“软件需求规格说明书”。④需求评审——评审需求分析的正确性、完整性和清晰性。

(3) 软件需求规格说明书：需求分析阶段的最后成果，是软件开发的重要文档之一。其作用有三：①便于用户、开发人员进行理解和交流；②反映出用户问题的结构，可以作为软件开发工作的基础和依据；③作为确认测试和验收的依据。软件需求规格说明书的内容主要包括概述、数据描述、功能描述、性能描述、参考文献和附录等。

3. 结构化分析方法

结构化分析(Structured Analysis，SA)方法是面向数据流进行需求分析的方法，采用自顶向下、逐层分解的方法，建立系统的处理流程，以数据流图和数据字典为主要工具，建立系统的逻辑模型。SA 方法的分析结果由以下几部分组成：一套分层的数据流图、一本数据词典、一组小说明。

1) 数据流图

数据流图(Data Flow Diagram，DFD)用来描述数据流从输入到输出的变换流程。它以图形的方式描绘数据在系统中流动和处理的过程，它只反映系统必须完成的逻辑功能，所以是一种功能模型。

DFD 的基本元素如图 13-7 所示。

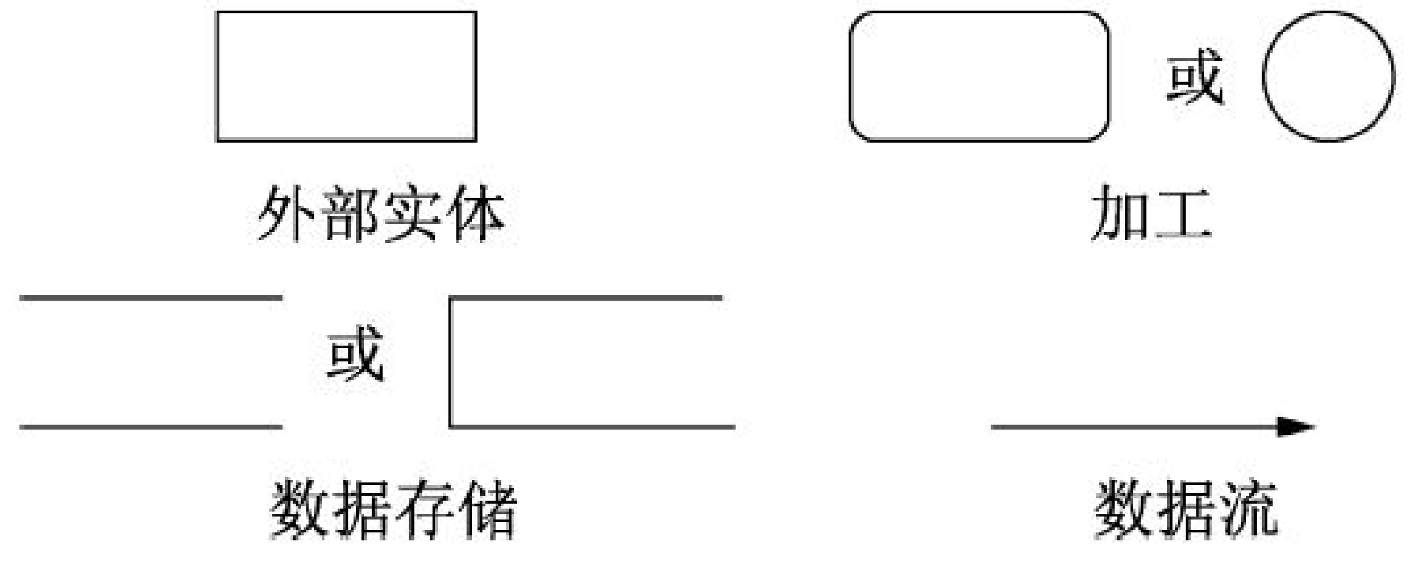


图 13-7　DFD 的基本元素

(1) 数据流：由一组固定成分的数据组成，表示数据的流向。

(2) 加工：描述了输入数据流到输出数据流之间的变换，也就是输入数据流经过某种处理后变成了输出数据流。

(3) 数据存储：用来表示暂时存储的数据，每个数据存储都有一个名字。

(4) 外部实体：它是指存在于软件系统之外的人员或组织。

2) 数据字典

数据流图仅描述了系统的“分解”，但没有对图中各成分进行说明。数据词典就是用来定义数据流图中的各个成分含义的。

数据字典有 4 类条目，包括数据流、数据项、数据存储和基本加工。

3) 加工逻辑的描述

加工逻辑的描述用来说明 DFD 中的数据加工的细节，表达“做什么”，而不是“怎样做”。描述工具有结构化语言、判定表和判定树。

4. 软件设计

从技术角度上讲，软件设计分成体系结构设计、数据设计、接口设计、过程设计 4 方面的工作。从管理角度上讲，软件设计分为概要设计、详细设计两个阶段。

1) 软件设计的基本原理

软件设计的基本原理如下。

(1) 模块化：将一个待开发的软件分解成若干个小的简单的部分——模块，每个模块可独立地开发、测试，最后组装成完整的程序。

(2) 抽象化：抽象是一种设计技术，抽出事物本质的共同特性而暂不考虑它的细节。

(3) 信息隐蔽：将每个程序的成分隐蔽或封装在一个单一的设计模块中，定义每一个模块时尽可能少地显露其内部的处理，可以提高软件的可修改性、可测试性和可移植性。

(4) 模块独立：每个模块完成一个相对独立的特定子功能，并且与其他模块之间的联系简单。衡量度量标准有两个：模块间的耦合和模块的内聚度。要想使模块独立性强必须做到高内聚低耦合。

2) 结构化设计方法

结构化设计(SD)方法是一种面向数据流的设计方法，它可以与 SA 方法链接。

在需求分析阶段，用 SA 方法产生了数据流图。面向数据流的设计能方便地将 DFD 转换成程序结构图。DFD 中从系统的输入数据流到系统的输出数据流的一连串连续变换形成了一条信息流。DFD 的信息流大体上可以分为两种类型，一种是变换流，另一种是事务流。

3) 软件详细设计

详细设计的任务是为软件结构图中的每一个模块确定实现算法和局部数据结构，用某种选定的表达工具表示算法和数据结构的细节。

结构化程序设计的基本要点如下。

- 采用自顶向下、逐步求精的程序设计方法。
- 使用顺序、选择、重复 3 种基本控制结构构造程序。
- 主程序员组的组织形式。

处理过程设计的关键是用一种合适的表达方法来描述每个模块的执行过程。这种表示方法应该简明、精确，并因此能直接导出用编程语言表示的程序。

- 程序流程图。其包括 3 种基本成分：加工步骤，用方框表示；逻辑条件，用菱形表示；控制流，用箭头表示。
- 盒图(N-S 图)。在 N-S 图中，每个处理步骤用一个盒子表示，盒子可以嵌套。盒子只能从上头进入，从下头走出，此外别无其他出入口，所以盒图限制了随意的控制转移，保证了程序的良好结构。
- 形式语言。形式语言是用来描述模块具体算法的非正式而比较灵活的语言。形式语言的优点是接近自然语言，所以易于理解。
- 决策树。决策树是一种图形工具，适合于描述加工中具有多个策略、每个策略和若干条件有关的逻辑功能。
- 决策表。决策表是一种图形工具，呈表形。决策表将比较复杂的决策问题简洁地描述出来。

4)　面向数据结构设计——Jackson 方法

面向数据结构设计是以数据结构作为设计的基础，它根据输入输出数据结构导出程序的结构，适用于规模不大的数据处理系统，Jackson 方法是一种典型的面向数据结构的设计方法。

5)　用户界面设计

用户界面设计是系统与用户之间的接口，也是控制和选择信息输入输出的主要途径。用户界面设计应坚持友好、简便、实用、易于操作的原则。

界面设计包括菜单方式、会话方式、操作提示方式以及操作权限管理方式等。

5. 面向对象分析与设计

1)　面向对象设计的基本概念

面向对象设计的基本概念如下。

(1)　对象：一组属性以及这组属性上的专用操作的封装体，通常由对象名、属性和操作这 3 个部分组成。属性表示该对象的状态，用户只能看见对象封装界面上的信息，对象的内部实现对用户是隐蔽的。封装目的是使对象的定义和实现分开。

(2)　类：一组具有相同属性和相同操作的对象的集合。一个类中的每个对象都是这个类的一个实例(Instance)。

(3)　继承：在某个类的层次关联中不同的类共享属性和操作的一种机制。一个父类可以有多个子类，这些子类都是父类的特例。父类描述了这些子类的公共属性的操作，子类中还可以定义它自己的属性和操作。一个子类只有唯一的一个父类，这种继承称为单一继承。一个子类有多个父类，可以从多个父类中继承特性，这种继承称为多重继承。

(4)　消息：对象间通信的手段。一个对象通过向另一个对象发送消息来请求其服务。消息通常包括接收对象名、调用的操作名和适当的参数(如有必要)。消息只告诉接收对象需要完成什么操作，但并不能指示接收者怎样完成操作。消息完全由接收者解释。接收者独立决定采用什么方法来完成所需的操作。

(5)　多态性：同一个操作作用于不同的对象可以有不同的解释，产生不同的执行结果。

(6)　继承性：是面向对象程序设计语言不同于其他语言的主要特点，是否建立了丰富的类库是衡量一个面向对象程序设计语言成熟与否的重要标志之一。

在面向对象的软件工程中，一个组件(Component)包含了一些协作的类的集合。

2) 面向对象分析与设计的基本概念

面向对象方法的基本思想是从现实世界中客观存在的事物出发来构造软件系统。面向对象分析(Object-Oriented Analysis，OOA)的目标是建立待开发软件系统的模型，面向对象设计(Object-Oriented Design，OOD)的目标是定义系统构造蓝图，设计分析模型和实现相应的源代码，在目标代码环境中这种源代码可被执行。

统一建模语言(UML)是面向对象软件的标准化建模语言。UML 由 3 个要素构成：UML 的基本构造块、支配这些构造块如何放置在一起的规则和运用于整个语言的一些公共机制。UML 的词汇表包含 3 种构造块：事务、关系和图。事务是对模型中最具代表性的成分的抽象，关系把事务结合在一起，图聚集了相关的事务。

- 事务，包括结构事务、行为事务、分组事务和注释事务。
- 关系，包括依赖、关联、泛化和实现。
- 图，包括类图、对象图、用例图、序列图、协作图、状态图、活动图、构件图和部署图。

13.3.1.2 项目管理基础知识

项目管理的核心内容就是在成本、质量、进度间的平衡，包括 POIM 4 个方面：Plan(计划)、Organize(组织)、Implement(实现)、Measurement(度量)。

1. 项目计划

项目计划的主要内容包括：①估算所需要的人力(通常以人月为单位)、项目持续时间(以年份或月份为单位)、成本(以元为单位)；②作出进度安排，分配资源，建立项目组织及任用人员(包括人员的地位、作用、职责、规章制度等)，根据规模和工作量估算分配任务；③进行风险分析，包括风险识别、风险估计、风险优化、风险驾驭策略、风险解决和风险监督，这些步骤贯穿在软件工程过程中；④制订质量管理指标；⑤编制预算和成本；⑥准备环境和基础设施等。

2. 质量计划、管理和评估

1) 软件质量度量模型

目前有多种软件质量模型。

(1) ISO/IEC 9126 软件质量模型。该模型由 3 个层次组成：第一层是质量特性，第二层是质量子特性，第三层是度量指标。

(2) Mc Call 软件质量模型。该模型从软件产品的运行、修正、转移等 3 个方面确定了 11 个质量特性。它给出了一个 3 层模型框架：第一层是质量特性；第二层是评价准则；第三层是度量指标。

2) 质量管理

软件管理通过制订质量方针、建立质量目标和标准(Target)，并在项目生命期内持续使用质量计划(Plan)、质量控制(Do)、质量保证(Check)和质量改进(Action)等措施来落实质量方针的执行，确保质量目标的实现，最大限度地使客户满意。

3) 软件质量评审

软件质量评审主要包括设计质量评审和程序质量评审。

3. 进度管理

软件开发项目的进度安排有两种方式。

(1) 系统最终交付日期已经确定，软件开发部门必须在规定期限内完成。

(2) 系统最终交付日期只确定了大致的年限，最后交付日期由软件开发部门确定。

进度安排的常用图形描述方法有甘特图(Gantt)和计划评审技术图(PERT)。

(1) Gantt(甘特)图：用水平线段表示任务的工作阶段；线段的起点和终点分别对应着任务的开工时间和完成时间；线段的长度表示完成任务所需的时间。

优点：能清晰地描述每个任务从何时开始、到何时结束以及各个任务之间的并行性。

缺点：不能清晰地反映出各任务之间的依赖关系，难以确定整个项目的关键所在，也不能反映计划中有潜力的部分。

(2) PERT 图：PERT 图是一个有向图，图中的有向弧表示任务，它可以标上完成该任务所需的时间；图中的节点表示流入节点的任务的结束，并开始流出节点的任务，这里把节点称为事件。只有当流入该节点的所有任务都结束时，节点所表示的事件才出现，流出节点的任务才可以开始。事件本身不消耗时间和资源，它仅表示某个时间点。每个事件有一个事件号和出现该事件的最早时刻和最迟时刻。每个任务还有一个松弛时间，表示在不影响整个工期的前提下，完成该任务有多少机动余地。松弛时间为 0 的任务构成了完成整个工程的关键路径。

PERT 图不仅给出了每个任务的开始时间、结束时间和完成该任务所需的时间，还给出了任务之间的关系，即哪些任务完成后才能开始另外一些任务，以及如期完成整个工程的关键路径。松弛时间则反映了完成某些任务时可以推迟其开始时间或延长其所需的完成时间。但是 PERT 图不能反映任务之间的并行关系。

4. 文档管理

文档是软件产品的一部分，没有文档的软件就不称其为软件。国家标准《计算机软件产品开发文件编制指南》(GB 8567—88)中规定，在一项软件开发过程中，一般地说应该产生 14 种文件。

5. 人员管理

可以按软件项目对软件人员分组，如需求分析组、设计组、编码组、测试组、维护组等。为了控制软件的质量，还可以有质量保证组。

6. 风险管理

风险分析在软件项目管理中具有决定性作用，它是贯穿在软件工程中的一系列风险管理步骤，其中包括风险识别、风险估计、风险管理策略、风险解决和风险监督。

7. 软件工具与软件开发环境

1) 软件工具

通常可将软件工具分为软件开发工具、软件维护工具和软件管理工具。

2) 软件开发环境

软件开发环境是支持软件产品开发的软件系统。它由工具集和环境集成机制两部分组成。工具集中还应该包含支持软件生存周期各阶段活动以及支持各种开发方法和开发模型的工具，能支持软件开发的全过程。而环境集成机制主要包含数据集成机制、控制集成机

制和界面集成机制等3方面内容。

8. 能力成熟度模型

能力成熟度模型(CMM)用于衡量软件企业的开发管理水平，它可作为软件发包方评估承包方执行能力的参考标准，也可以被软件企业作为软件过程改进工作的参考模型。CMM将软件过程的成熟度分为5个等级：初始级、可重复级、已定义级、已管理级、优化级。

13.3.1.3 软件的测试与调试

1. 软件测试的目的

软件测试的目的是尽可能多地发现软件产品(主要是指程序)中的错误和缺陷。成功的测试是发现了至今未发现的错误的测试。

2. 软件测试的过程

一个规范的软件测试过程通常包括制订测试计划、编制测试大纲、根据测试大纲设计和生成测试用例、实施测试和生成测试报告。

3. 软件测试的方法

软件测试的关键是测试用例的设计。软件测试的种类大致可分为人工测试和动态测试，动态测试方法中又根据测试用例的设计方法不同，分为白盒测试和黑盒测试。

1) 白盒测试

白盒测试法需要了解程序内部的结构，测试用例是根据程序的内部逻辑来设计的。白盒测试法主要用于软件的单元测试。

白盒测试的基本原则如下。

(1) 保证所测模块中每一个独立路径至少执行一次。

(2) 保证所测模块所有判断的每一个分支至少执行一次。

(3) 保证所测模块每一个循环都在边界条件和一般条件至少执行一次。

(4) 验证所有内部数据结构的有效性。

白盒测试法常用的技术是逻辑覆盖。主要的覆盖标准有6种，强度由低到高依次是语句覆盖、判定覆盖、条件覆盖、判定/条件覆盖、条件组合覆盖、路径覆盖。

2) 黑盒测试

黑盒测试是对软件已经实现的功能是否满足需求进行测试和验证。黑盒测试不关心程序内部的逻辑，只是根据程序的功能说明来设计测试用例。黑盒测试法主要用软件的确认测试。

测试方法有以下几种。

(1) 等价类划分：把输入数据划分成若干个有效等价类和若干个无效等价类，然后设计测试用例覆盖这些等价类。

(2) 边界值分析：对各种输入、输出范围的边界情况设计测试用例的方法。这是因为程序中在处理边界情况时出错的概率比较大。

(3) 错误猜测：根据经验或直觉推测程序中可能存在的各种错误。

(4) 因果图：根据输入条件与输出结果之间的因果关系来设计测试用例。

4. 软件测试步骤

软件测试的步骤如下。

(1) 单元测试：其也称模块测试，主要发现编码和详细设计中产生的错误，通常采用白盒测试。放在编码阶段，由程序员自己来完成，检查它是否实现了详细设计说明书中规定的模块功能和算法。单元测试的测试计划是在详细设计阶段完成。

(2) 集成测试：其也称组装测试，对由各模块组装而成的程序进行测试，主要检查模块间的接口和通信。集成测试主要发现设计阶段产生的错误，通常采用黑盒测试或灰盒测试。集成的方式可分成非渐增式集成和渐增式集成。集成测试的测试计划是在概要设计阶段完成。

(3) 确认测试：检查软件的功能、性能及其他特征是否与用户的需求一致，它是以需求规格说明书(即需求规约)作为依据的测试。确认测试通常采用黑盒测试，其测试计划是在需求分析阶段完成。

(4) 系统测试：把已经过确认的软件纳入实际运行环境中，与其他系统成分组合在一起进行测试。主要内容包括恢复测试、安全测试、强度测试、性能测试、可靠性测试、安装测试等。

5. 软件调试

软件调试是在进行了成功的测试之后才开始的工作。其任务是进一步诊断和改正程序中潜在的错误。调试由两部分组成：确定错误的确切性质和位置、修改程序(设计、编码)。目前常用的调试方法有以下 5 种：试探法、回溯法、对分查找法、归纳法、演绎法。

13.3.1.4　系统维护

1. 系统维护的内容

系统维护包括以下内容。

(1) 硬件维护。硬件维护应由专职的硬件维护人员来负责。主要有两种类型的维护活动：一种是定期的设备保养性维护，另一种是突发性的故障维护。

(2) 软件维护。软件维护主要是根据需求变化或硬件环境的变化对应用程序进行部分或全部的修改。

(3) 数据维护。数据维护主要是由数据库管理员来负责，主要负责数据库的安全性和完整性以及进行并发性控制。

2. 软件维护的内容

软件维护的内容包括正确性维护、适应性维护、完善性维护和预防性维护等。

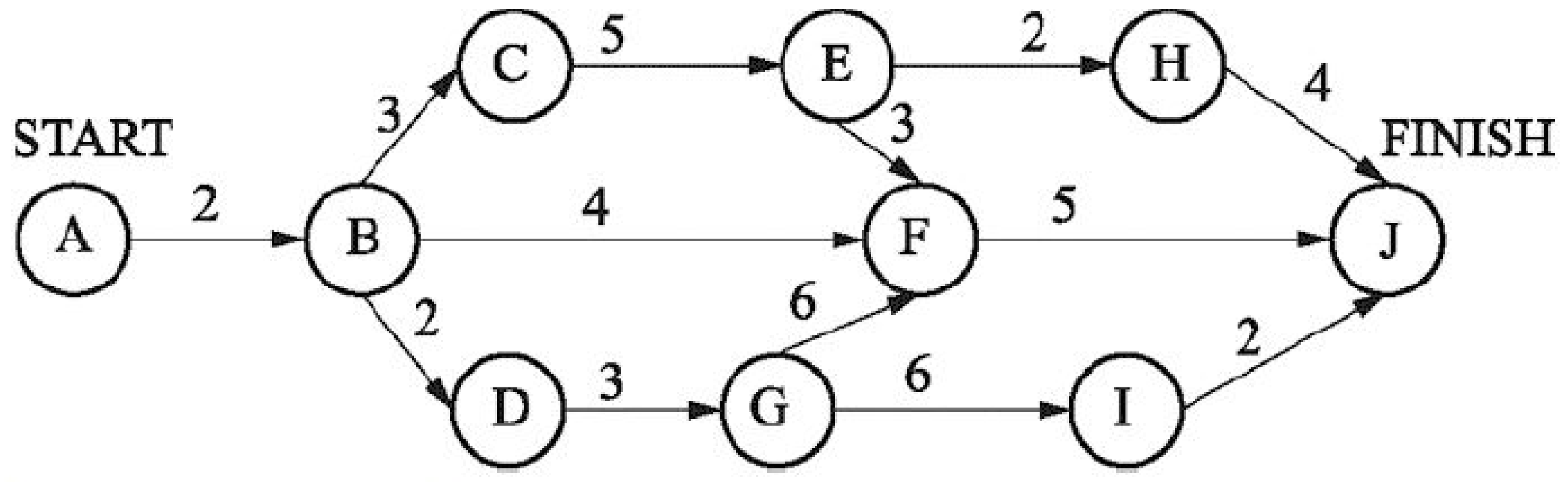
3. 软件可维护性的质量特性

软件可维护性可以用以下 7 个质量特性来衡量：可理解性、可测试性、可修改性、可靠性、可移植性、可使用性和效率。

13.3.2 典型例题分析

例 13-28 某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示活动的持续时间(天)。完成该项目的最少时间为 __(7)__ 天。

由于某种原因，现在需要同一个开发人员完成 BC 和 BD，完成该项目需最少时间为 __(8)__ 天。(2017 年下半年真题 7、8)



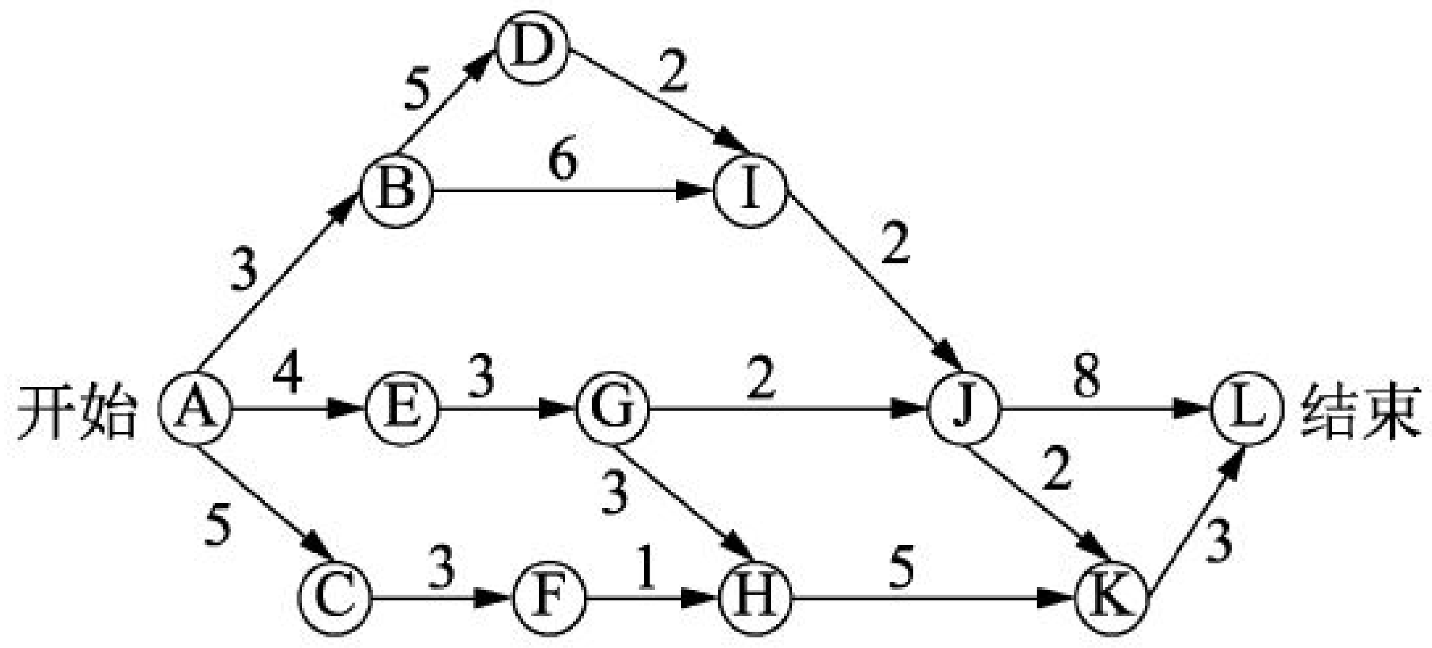
(7)、(8) A.11　　B. 18　　C. 20　　D. 21

解析： 本题的关键路径可知为 ABCEFJ 和 ABDGFJ，都是 18。

若由同一个开发人员完成 BC 和 BD，两个任务不可能并行工作，故存在一个先后问题。若先完成 BD，则相当于 BC 用时 3+2=5 天，则总工期为 20 天；若先完成 BC，则 BD 用时 2+3=5 天，总工期为 21 天。所以至少需要 20 天。

答案： (7) B　(8) C

例 13-29 某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示活动的持续时间(天)，则完成该项目的最少时间为 __(4)__ 天。活动BD和HK最早可以从第 __(5)__ 天开始。(活动AB、AE和AC最早从第1天开始)(2017 年上半年真题 4、5)



(4)　A. 17　　B. 18　　C. 19　　D. 20

(5)　A. 3 和 10　　B. 4 和 11　　C. 3 和 9　　D. 4 和 10

解析： 本题考查的是 PERT 图。要求完成该项目的最少时间即为求该项目的关键路径，关键路径是所需时间最长的任务流：ABDIJL，20 天。

活动 BD 在活动 AB 完成后才能开始进行，而活动 AB 需要 3 天的时间，故活动 BD 可在第四天的时候开展。活动 HK 最早开始需要 AEGH(10 天)和 ACFH(9 天)均要完成后才能开始，故其应在第十一天开展。

答案： (4) D　(5) B

例 13-30 在敏捷过程的开发方法中， __(6)__ 使用了迭代的方法，其中，把每段时间(30 天)一次的迭代称为一个“冲刺”，并按需求的优先级别来实现产品，多个自组织和自治的

小组并行地递增实现产品。(2016 年下半年真题 6)

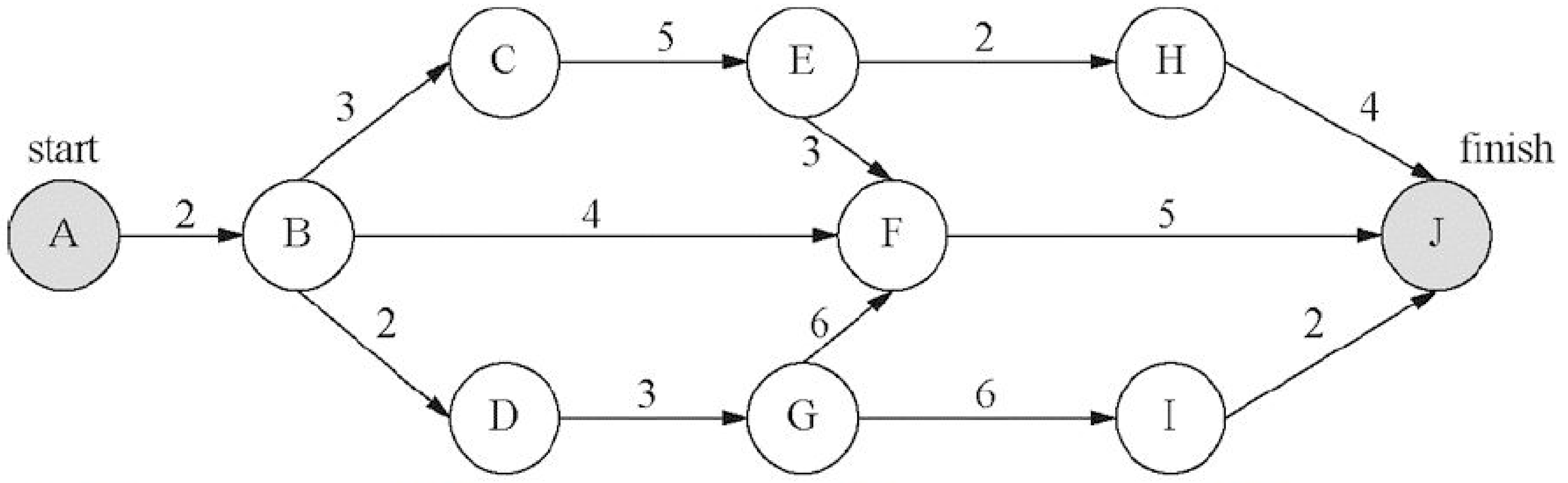
A. 极限编程(XP)　　B. 水晶法

C. 并列争球法　　D. 自适应软件开发

解析：敏捷开发是针对传统的瀑布开发模式的弊端而产生的一种新的开发模式，目标是提高开发效率和响应能力。常用的开发方法就是极限编程(XP)、水晶法、并列争球法、自适应软件开发这 4 种。极限编程(XP)：激发软件人员的创造性，管理负担最小。水晶法：每个项目都需要不同策略、约定和方法论。并列争球法：迭代，冲刺，多个自组织的小组并行地递增实现产品。自适应软件开发：使命作为指导，人员协作，团队组织设立项目的目标。

答案：C

例 13-31　某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示相应活动的持续时间(天)，则完成该项目的最少时间为__(7)__天。活动 BC 和 BF 最多可以晚开始__(8)__天而不会影响整个项目的进度。(2016 年下半年真题 7、8)



(7) A. 11　　B. 15　　C. 16　　D. 18

(8) A. 0 和 7　　B. 0 和 11　　C. 2 和 7　　D. 2 和 11

解析：在 PERT 图中，从 start 到 finish 最长的路径就是关键路径，也是完成该项目的最少时间。分析该活动图可知，关键路径为 ABCEFJ 和 ABDGFJ，均为 18 天。BC 所在的路径就是关键路径，松弛时间为 0; BF 所在的路径最长时间为 11 天，则松弛时间为 18−11=7 天，故 BF 可以晚开始 7 天。

答案：(7) D　(8) A

例 13-32　在结构化分析中，用数据流图描述__(7)__。当采用数据流图对一个图书馆管理系统进行分析时，__(8)__是一个外部实体。(2016 年上半年真题 7、8)

(7) A. 数据对象之间的关系，用于对数据建模

B. 数据在系统中如何被传送或变换，以及如何对数据流进行变换等功能或子功能，用于对功能建模

C. 系统对外部事件如何响应，如何动作，用于对行为建模

D. 数据流图中的各个组成部分

(8) A. 读者　　B. 图书　　C. 借书证　　D. 借阅

解析：数据流图(Data Flow Diagram，DFD)从数据传递和加工角度，以图形方式来表达系统的逻辑功能、数据在系统内部的逻辑流向和逻辑变换过程。数据流图是结构化系统分析方法的主要表达工具及用于表示软件模型的一种图示方法。外部实体是指独立于系统而

存在的，但又和系统有联系的实体，它表示数据的外部来源和最后去向。显然，读者是图书馆管理系统的一个外部实体。

答案：**(7)** B　(8) A

例 13-33　以下关于软件项目管理中人员管理的叙述，正确的是__(5)__。(2015 年下半年真题 5)

A. 项目组成员的工作风格也应该作为组织团队时要考虑的一个要素

B. 鼓励团队的每个成员充分地参与开发过程的所有阶段

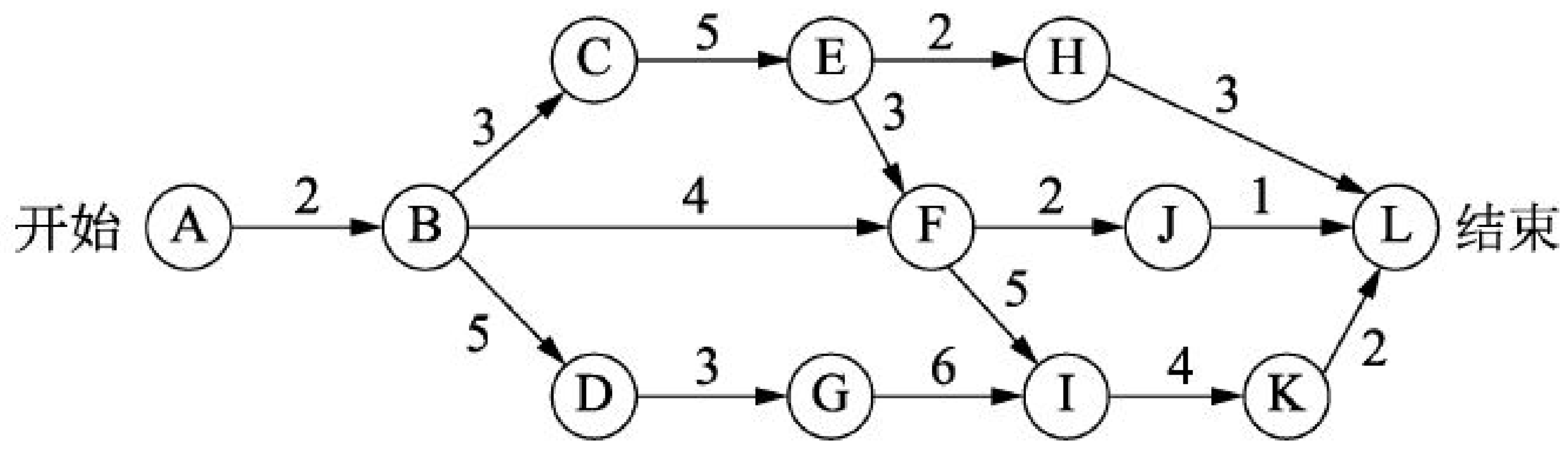
C. 仅根据开发人员的能力来组织开发团队

D. 若项目进度滞后于计划，则增加开发人员一定可以加快开发进度

解析：在软件项目中开发人员管理是核心的资源，其中人员的配置、调度安排贯穿整个软件项目过程。人员安排的组织管理是否得当，对软件项目成功起到决定性的作用。在软件项目初始阶段，要根据工作量大小，所需的专业技能类型，团队成员能力水平、性格和开发经验，组建开发小组。整个项目被分解，项目中的成员根据所述的专业组的职能承担项目的相应任务。当项目进度滞后于计划时，下意识的反应往往是增加人力，这是不太可取的，因为在项目中新加入的程序员往往更难融入项目中，所花费的时间代价会更大。

答案：A

例 13-34　某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示活动，边上的数字表示该活动所需的天数，则完成该项目的最少时间为__(6)__天。活动 BD 最多可以晚__(7)__天开始而不会影响整个项目的进度。(2015 年下半年真题 6、7)



(6)　A. 9　　B. 15　　C. 22　　D. 24

(7)　A. 2　　B. 3　　C. 5　　D. 9

解析：本题关键路径为：A→B→C→E→F→I→K→L，是活动图中花费时间最长的活动的序列，长度为 24。BD 在路径 A→B→D→G→I→K→L，长度为 22，比关键路径短 2，因此，要想不影响整个项目的进度，活动 BD 最多可以晚 2 天开始。

答案：(6) D　(7) A

13.3.3　同步练习

1.　以下关于结构化开发方法的叙述中，不正确的是________。

　A. 总的指导思想是自顶向下，逐层分解

　B. 基本原则是功能的分解与抽象

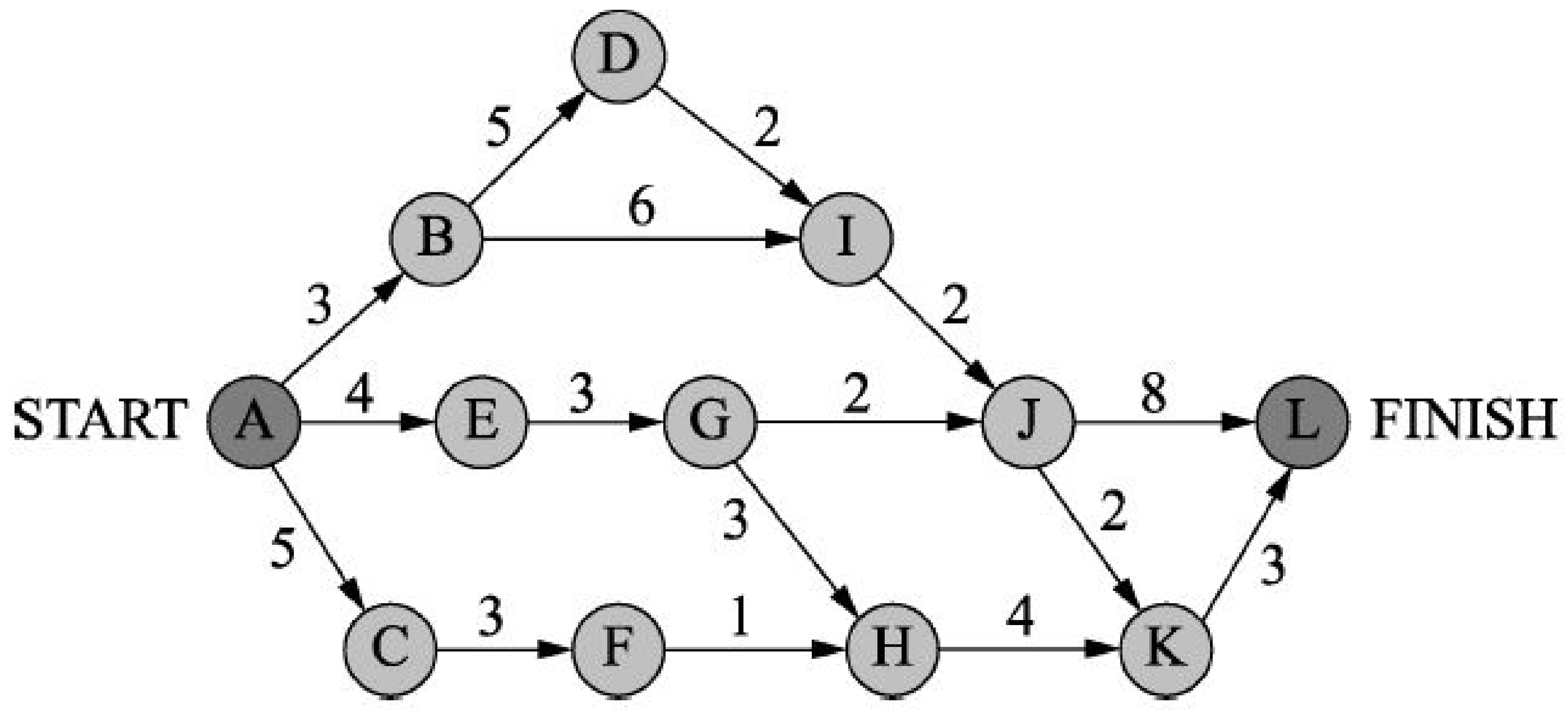
　C. 与面向对象开发方法相比，更适合大规模、特别复杂的项目

　D. 特别适合于数据处理领域的项目

2.　下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示活动，边的权重表示活动的持续时间，则里程碑__(1)__在关键路径上，活动 GH 的松弛时间是__(2)__。

(1)　A. B　　B. E　　C. C　　D. K

(2)　A. 0　　B. 1　　C. 2　　D. 3



3.　将高级语言源程序翻译成机器语言程序的过程中，常引入中间代码。以下关于中间代码的叙述中，不正确的是________。

A. 中间代码不依赖于具体的机器

B. 使用中间代码可提高编译程序的可移植性

C. 中间代码可以用树或图表示

D. 中间代码可以用栈或队列表示

4.　以下关于进度管理工具 Gantt 图的叙述中，不正确的是________。

A. 能清晰地表达每个任务的开始时间、结束时间和持续时间

B. 能清晰地表达任务之间的并行关系

C. 不能清晰地确定任务之间的依赖关系

D. 能清晰地确定影响进度的关键任务

13.3.4　同步练习参考答案

1. C　　2. (1) A　(2) D　　3. D　　4. D

13.4　标准化和信息化

13.4.1　考点辅导

13.4.1.1　标准化知识

制定标准的目的是获得最佳秩序、促进最佳社会效益。制定标准应遵循的原则是：要从全局利益出发，认真贯彻国家技术经济政策；充分满足使用要求；有利于促进科学技术的发展。

标准化的主要形式有简化、统一化、系列化、通用化及组合化。

1. 标准的代号和编号

1)　国内、国外标准代号及编号

基本结构为：标准代号＋专业类号＋顺序号＋年代号

2) 我国标准代号及编号

基本结构为：标准代号＋标准发布顺序号＋标准发布年号

2. 标准的有效期

标准的有效期是指自标准实施之日起，至标准复审重新确认、修订或废止的时间。ISO 标准每 5 年复审一次，平均标龄为 4.92 年。我国在国家标准管理办法中规定国家标准实施 5 年内要进行复审，即国家标准有效期一般为 5 年。

13.4.1.2 知识产权

1. 知识产权的概念

知识产权又称为智慧财产权，是指人们因通过自己的智力活动创造的成果和在经营管理活动中获得的经验、知识而依法享有的权利。传统的知识产权可分为“工业产权”和“著作权”(版权)两类。

工业产权包括专利、实用新型、工业品外观设计、商标、服务标记、厂商名称、产地标记或原产地名称、制止不正当竞争等项内容。此外，商业秘密、微生物技术、遗传基因技术等也属于工业产权保护的对象。

著作权(又称为版权)是指作者对其创作的作品享有的人身权和财产权，包括发表权、署名权、修改权和保护作品完整权、复制权、发行权、出租权、展览权、表演权、放映权、广播权、信息网络传播权、摄制权、改编权、翻译权、汇编权、应当由著作权人享有的其他权利。著作权的保护对象包括文学、科学和艺术领域内的一切作品。

2. 计算机软件著作权的主体与客体

计算机软件著作权的主体指享有著作权的人，包括公民、法人和其他组织。

计算机软件的客体指著作权法保护的计算机软件著作权的范围。根据《中华人民共和国著作权法》第 3 条和《计算机软件保护条例》第 2 条的规定，著作权法保护的是计算机程序及其有关文档。

3. 计算机软件著作权的权利

1) 计算机软件的著作人身权

计算机软件的著作人身权主要包括两种权利：人身权(精神权利)和财产权(经济权利)。软件著作人还享有发表权和开发者身份权。发表权是指是否公布软件作品的权利。开发者身份权又称为署名权，指软件作者在作品中署自己名字的权利。

2) 计算机软件的著作财产权

计算机软件的著作财产权是指能够给著作权人带来经济利益的权利。通常是指由软件著作权人控制和支配，并能够为权利人带来一定经济效益的权利。主要内容有使用权、复制权、修改权、发行权、翻译权、注释权、信息网络传播权、出租权、使用许可权和获得报酬权、转让权等。

4. 计算机软件著作权的保护期

自软件开发完成之日起，计算机软件著作权的保护期为 50 年。保护期满，除开发者身份权外，其他权利终止。计算机软件著作权人的单位终止和计算机软件著作权人的公民死

亡且无合法继承人时，除开发者身份权外的其他权利进入公有领域。

5. 计算机软件著作权的归属

1)　软件著作权归属的基本原则

我国《中华人民共和国著作权法》规定软件著作权属于作者。《计算机软件保护条例》规定软件著作权属于软件开发者。

2)　职务开发软件著作权的归属

当公民作为某单位的雇员时，如其开发的软件属于执行本职工作的结果，则软件著作权应当归单位享有。若开发的软件不是执行本职工作的结果，其著作权不属于单位享有；如果该雇员主要使用了单位的设备，按照《计算机软件保护条例》第 13 条第 3 款的规定，不能属于该雇员所有。

3)　合作开发软件著作权的归属

由两个或两个以上的公民、法人或其他组织订立协议，共同开发完成的软件属于合作开发的软件，其著作权的归属一般是共同享有，合作开发者不能单独行使转让权。如果有软件著作权的协议，则按照协议确定软件著作权的归属。

4)　委托开发的软件著作权的归属

受委托创作的软件，著作权的归属由委托人和受托人通过合同约定。合同未作明确约定或者没有订立合同的，著作权属于受托人。

5)　接受任务开发的软件著作权的归属

接受任务开发的软件著作权归属在合同中明确约定的，按照合同约定实行；未明确约定的，著作权属于实际完成软件开发的单位。

6)　计算机软件著作权主体变更后软件著作权的归属

因主体变更引起的变化有以下几种。

- 公民继承的软件权利归属：合法继承人享有除署名权外的其他权利。
- 单位变更后软件权利归属：由承受其权利义务的法人或者其他组织享有；没有承受其权利义务的法人或者其他组织的，由国家享有。
- 权利转让后的软件著作权归属：权利转让根据签订的合同规定各方的权利。
- 司法判决、裁定引起的软件著作权归属问题：根据法律的判决来执行。
- 保护期届满权利丧失。

6. 软件著作权侵权的法律责任

需要承担民事责任的侵权行为有：未经软件著作权人的许可发表或登记其软件的；将他人的软件当作自己的软件发表或登记的；未经合作者许可，将与他人合作开发的软件当作自己独立完成的作品发表或者登记的；在他人开发的软件上署名或者更改他人开发的软件上的署名的；未经软件著作权人或者其合法受让者的许可，修改或翻译其软件的；其他侵犯软件著作权的行为。

需要承担行政责任的侵权行为有：复制或部分复制著作权人软件的；向公众发行、出租著作权人软件的；故意避开或者破坏著作权人为保护其软件而采取的技术措施的；故意删除或者改变软件权利管理电子信息的；许可他人行使或者转让著作权人的软件著作权的。

侵权行为触犯法律的，侵权者承担相应的刑事责任。

7. 计算机软件的商业秘密权

我国《中华人民共和国反不正当竞争法》中商业秘密被定义为“不为公众所熟悉的、能为权利人带来经济效益、具有实用性并经权利人采取保密措施的技术信息和经营信息”，其中经营秘密和技术秘密是商业秘密的基本内容。

根据我国《中华人民共和国反不正当竞争法》第 10 条规定，侵犯计算机软件商业秘密的具体表现形式主要有以下几种。

(1) 以盗窃、利诱、胁迫或以其他不正当手段获取权利人的计算机软件商业秘密。

(2) 披露、使用或允许他人使用以不正当手段获取的权利人的计算机软件商业秘密。

(3) 违反约定或违反权利人有关保守商业秘密的要求，披露、使用或允许他人使用其掌握的计算机软件商业秘密的行为。

(4) 第三方在明知前述违法行为的情况下，仍然从侵权人那里获取或使用他人计算机软件商业秘密的行为。该行为属于间接侵权。

8. 专利权

发明创造是产生专利权的基础。发明创造是指发明、实用新型和外观设计，是我国专利法主要保护的对象。《中华人民共和国专利法实施细则》第 2 条第 1 款规定：“专利法所称的发明，是指对产品、方法或者其改进所提出的新的技术方案。” 一项发明或者实用新型获得专利的实质条件为新颖性、创造性和实用性。

专利申请采用书面形式，一项专利申请文件只能申请一项专利。发明或者实用新型的专利申请文件包括请求书、说明书、说明书摘要、权利要求书。外观设计专利申请文件包括请求书、图片或照片。两个或两个以上的人就同样的发明创造申请专利的，专利权授予最先申请人。专利局收到发明专利申请后，一个必要程序是初步审查，经初步审查认为符合本法要求的，自申请之日起满 18 个月，即行公布，专利局可根据申请人的请求，早日公布其申请。自申请之日起 3 年内，专利局可根据申请人随时提出的请求，对其申请进行实质审查。实质审查是依法审查专利的新颖性、创造性和实用性。

根据我国专利法的规定，发明专利的保护期限为 20 年，实用新型和外观设计专利为 10 年。

13.4.2 典型例题分析

例 13-35 李某购买了一张有注册商标的应用软件光盘，则李某享有__(6)__。(2017 年下半年真题 6)

A. 注册商标专用权　　B. 该光盘的所有权

C. 该软件的著作权　　D. 该软件的所有权

解析： 购买软件仅拥有该软件的使用权。

答案： B

例 13-36 根据我国商标法，下列商品中必须使用注册商标的是__(9)__。(2017 年上半年真题 9)

A. 医疗仪器　　B. 墙壁涂料　　C. 无糖食品　　D. 烟草制品

解析：目前根据我国法律法规的规定必须使用注册商标的是烟草类商品。《烟草专卖法》(1991 年 6 月 29 日通过，1992 年 1 月 1 日施行)第二十条规定：“卷烟、雪茄烟和有包装的烟丝必须申请商标注册，未经核准注册的，不得生产、销售。禁止生产、销售假冒他人注册商标的烟草制品。”

答案：D

例 13-37　甲、乙两人在同一天就同样的发明创造提交了专利申请，专利局将分别向各申请人通报有关情况，并提出多种可能采用的解决办法。以下说法中，不可能采用的是__(10)__(2017 年上半年真题 10)

A. 甲、乙作为共同申请人

B. 甲或乙一方放弃权利并从另一方得到适当的补偿

C. 甲、乙都不授予专利权

D. 甲、乙都授予专利权

解析：专利权谁先申请谁拥有，同时申请则协商归属，但不能够同时驳回双方的专利申请。按照专利法的基本原则，对于同一个发明只能授予一个专利权。

答案：D

例 13-38　甲、乙两厂生产的产品类似，且产品都拟使用“B”商标。两厂于同一天向商标局申请商标注册，且申请注册前两厂均未使用“B”商标。此情形下，__(10)__能核准注册。(2016 年下半年真题 10)

A. 甲厂　　B. 由甲、乙厂抽签确定的厂

C. 乙厂　　D. 甲、乙两厂

解析：《商标法实施条例》第十九条:

两个或者两个以上的申请人，在同一种商品或者类似商品上，分别以相同或者近似的商标在同一天申请注册的，各申请人应当自收到商标局通知之日起 30 日内提交其申请注册前在先使用该商标的证据。同日使用或者均未使用的，各申请人可以自收到商标局通知之日起 30 日内自行协商，并将书面协议报送商标局；不愿协商或者协商不成的，商标局通知各申请人以抽签的方式确定一个申请人，驳回其他人的注册申请。商标局已经通知但申请人未参加抽签的，视为放弃申请，商标局应当书面通知未参加抽签的申请人。

答案：B

例 13-39　某软件公司参与开发管理系统软件的程序员张某，辞职到另一公司任职，于是该项目负责人将该管理系统软件上开发者的署名更改为李某(接张某工作)。该项目负责人的行为__(3)__。(2016 年上半年真题 3)

A. 侵犯了张某开发者身份权(署名权)

B. 不构成侵权，因为程序员张某不是软件著作权人

C. 只是行使管理者的权利，不构成侵权

D. 不构成侵权，因为程序员张某现已不是项目组成员

解析：张某参加某软件公司开发管理系统软件的工作，属于职务行为，该管理系统软件的著作权归属公司所有，但根据《著作权法》，张某拥有该管理系统软件的署名权。而该项目负责人将作为软件系统开发者之一的张某的署名更改为他人，根据《计算机软件保

护条例》第 23 条第 4 款的规定，项目负责人的行为侵犯了张某的开发者身份权及署名权。

答案：A

例 13-40 王某在其公司独立承担了某综合信息管理系统软件的程序设计工作。该系统交付用户、投入试运行后，王某辞职，并带走了该综合信息管理系统的源程序，拒不交还公司。王某认为，综合信息管理系统源程序是他独立完成的，他是综合信息管理系统源程序的软件著作权人。王某的行为 (10) 。(2015 年下半年真题 10)

A. 侵犯了公司的软件著作权　　B. 未侵犯公司的软件著作权

C. 侵犯了公司的商业秘密权　　D. 不涉及侵犯公司的软件著作权

解析：王某完成的软件是在职期间开发的，因此该软件的著作权归单位享有。他的行为侵犯了公司的著作权。

答案：A

例 13-41 王某是某公司的软件设计师，每当软件开发完成后均按公司规定编写软件文档，并提交公司存档，那么该软件文档的著作权 (9) 享有。(2015 年上半年真题 9)

A. 应由公司　　B. 应由公司和王某共同

C. 应由王某　　D. 除署名权以外，著作权的其他权利由王某

解析：王某编写的软件文档属于职务作品，职务作品的著作权应由公司享有。

答案：A

13.4.3 同步练习

1. 甲公司接受乙公司委托开发了一项应用软件，双方没有订立任何书面合同。在此情形下，________享有该软件的著作权。

   A. 甲公司　B. 甲、乙公司共同　C. 乙公司　D. 甲、乙公司均不

2. 王某买了一幅美术作品原件，则他享有该美术作品的________。

   A. 著作权　　B. 所有权

   C. 展览权　　D. 所有权与其展览权

13.4.4 同步练习参考答案

1. A　2. D

13.5 本 章 小 结

本章知识点在 2014 年的新大纲中改动不大，主要是删除了部分知识点，还有一些表述方式的调整。

本章要求考生掌握计算机硬件基础、操作系统、系统开发和运行以及标准化和信息化等基础知识。

本章相关知识点在历次考试中都会有所涉及，分值在 10 分左右。对本章的学习关键要

掌握大纲的精神，明确考试范围，以典型例题为主线，抓住重点，学会取舍。本章每节都组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。

13.6　达标训练题及参考答案

13.6.1　达标训练题

1. 常用的虚拟存储器由________两级存储器组成。

A. 主存-辅存　　B. 主存-网盘
C. Cache-主存　　D. Cache-硬盘

2. 中断向量可提供________。

A. I/O 设备的端口地址　　B. 所传送数据的起始地址
C. 中断服务程序的入口地址　　D. 主程序的断点地址

3. 为了便于实现多级中断，使用________来保护断点和现场最有效。

A. ROM　　B. 中断向量表　　C. 通用寄存器　　D. 堆栈

4. DMA 工作方式下，在________之间建立直接的数据通信。

A. CPU 与外设　　B. CPU 与主存
C. 主存与外设　　D. 外设与外设

5. 地址编号从 80000H～BFFFFH 且按字节编址的内存容量为 (1) KB，若用 16K×4bit 的存储器芯片构成该内存，共需 (2) 片。

(1) A. 128　　B. 256　　C. 512　　D. 1024
(2) A. 8　　B. 16　　C. 32　　D. 64

6. 在 CPU 中，________不仅要保证指令的正确执行，还要能够处理异常事件。

A. 运算器　　B. 控制器　　C. 寄存器组　　D. 内部总线

7. 计算机中主存储器主要由存储体、控制线路、地址寄存器、数据寄存器和______组成。

A. 地址译码电路　　B. 地址和数据总线
C. 微操作形成部件　　D. 指令译码器

8. 以下关于数的定点表示或浮点表示的叙述中，不正确的是______。

A. 定点表示法表示的数(称为定点数)常分为定点整数和定点小数两种
B. 定点表示法中，小数点需要占用一个存储位
C. 浮点表示法用阶码和尾数来表示数，称为浮点数
D. 在总位数相同的情况下，浮点表示法可以表示更大的数

9. X、Y 为逻辑变量，与逻辑表达式 $X+\overline{X}Y$ 等价的是______。

A. $X+\overline{Y}$　　B. $\overline{X}+\overline{Y}$　　C. $\overline{X}+Y$　　D. $X+Y$

10. 位于 CPU 与主存之间的高速缓冲存储器(Cache)用于存放部分主存数据的副本，主存地址与 Cache 地址之间的转换工作由________完成。

A. 硬件　　B. 软件　　C. 用户　　D. 程序员

11. 内存单元按字节编址，地址 0000A000H～0000BFFFH 共有________个存储单元。

A. 8192K　　B. 1024K　　C. 13K　　D. 8K

12. 相联存储器按______访问。

A. 地址　　B. 先入后出的方式

C. 内容　　D. 先入先出的方式

13. 若 CPU 要执行的指令为：MOV R1，#45(即将数值 45 传送到寄存器 R1 中)，则该指令中采用的寻址方式为______。

A. 直接寻址和立即寻址　　B. 寄存器寻址和立即寻址

C. 相对寻址和直接寻址　　D. 寄存器间接寻址和直接寻址

14. 假设某分时系统采用简单时间片轮转发，当系统中的用户数为 n，时间片为 q 时，系统对每个用户的响应时间 T 为________。

A. n　　B. q　　C. $n\times q$　　D. $n+q$

15. 若要访问文件的逻辑块号分别为 5 和 518，则系统应分别采用________。

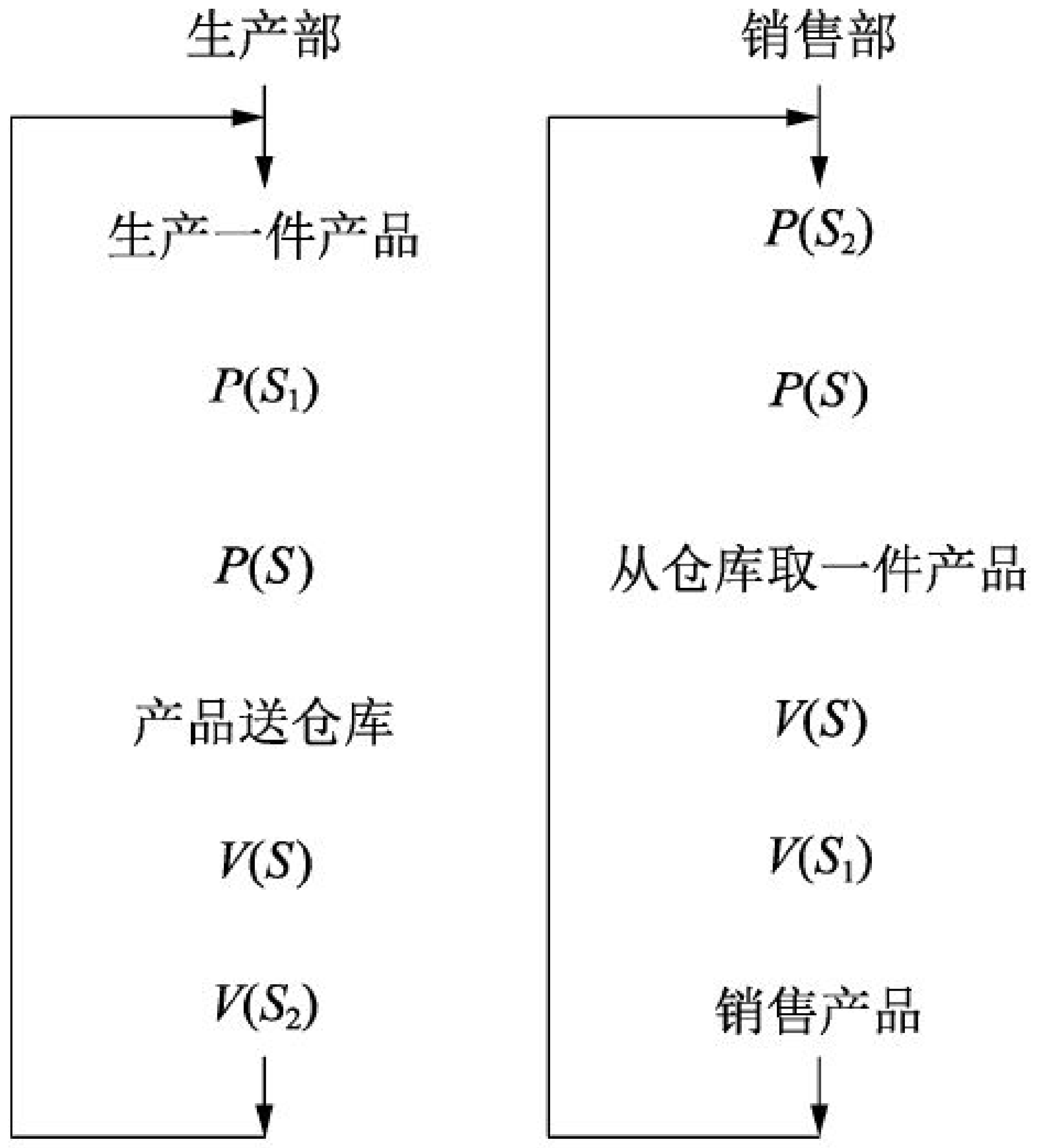
A. 直接地址索引和一级间接地址索引

B. 直接地址索引和二级间接地址索引

C. 一级间接地址索引和二级间接地址索引

D. 一级间接地址索引和一级间接地址索引

16. 某企业有生产部和销售部，生产部负责生产产品并送入仓库，销售部从仓库取出产品销售。假设仓库可存放 n 件产品。用 PV 操作实现它们之间的同步过程如下图所示。



图中信号量 S_1 和 S_2 为同步信号量，初值分别为 n 和 0；S 是一个互斥信号量，初值为______。

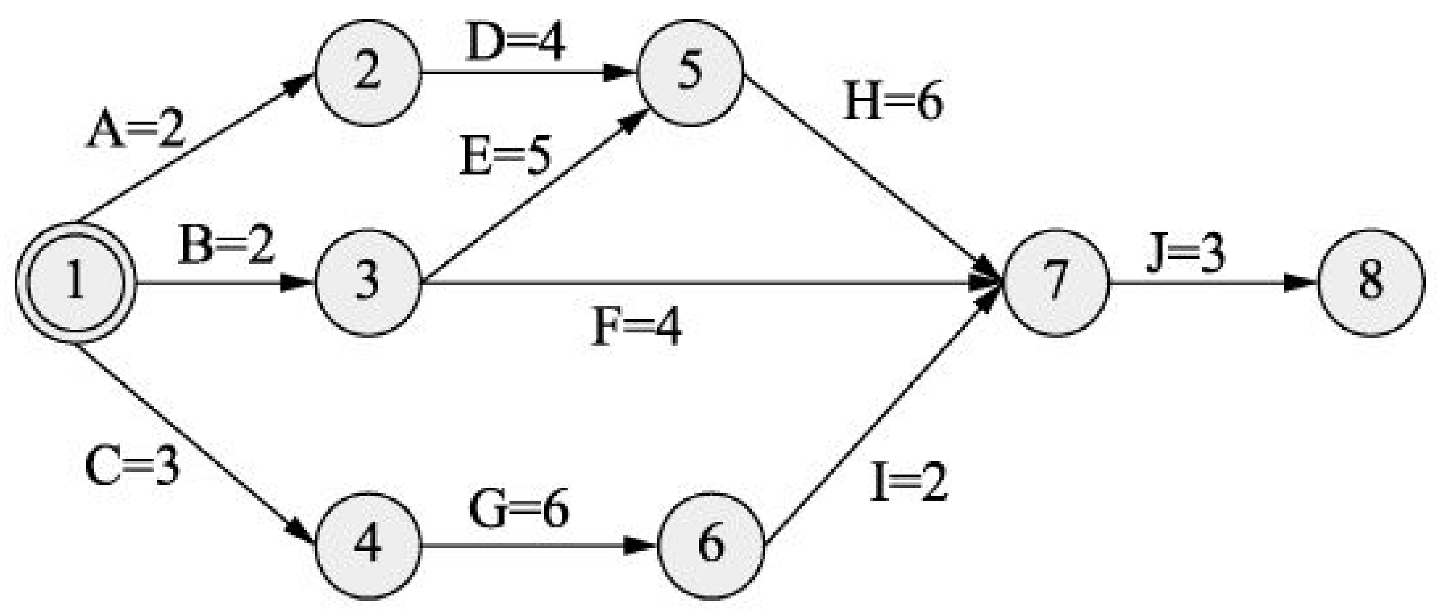
A. 0　　B. 1　　C. n　　D. −1

17. 在进行进度安排时，PERT 图不能清晰地描述__(1)__，但可以给出哪些任务完成后才能开始另一任务。某项目 X 包含任务 A、B、…、J，其 PERT 如下图所示(A=1 表示该任务 A 的持续时间是 1 天)，则项目 X 的关键路径是__(2)__。

(1) A. 每个任务从何时开始　　B. 每个任务到何时结束

C. 各任务之间的并行情况　　D. 各任务之间的依赖关系

(2) A. A-D-H-J　　B. B-E-H-J　　C. B-F-J　　D. C-G-I-J



18. 在软件设计阶段，划分模块的原则是，一个模块的______。

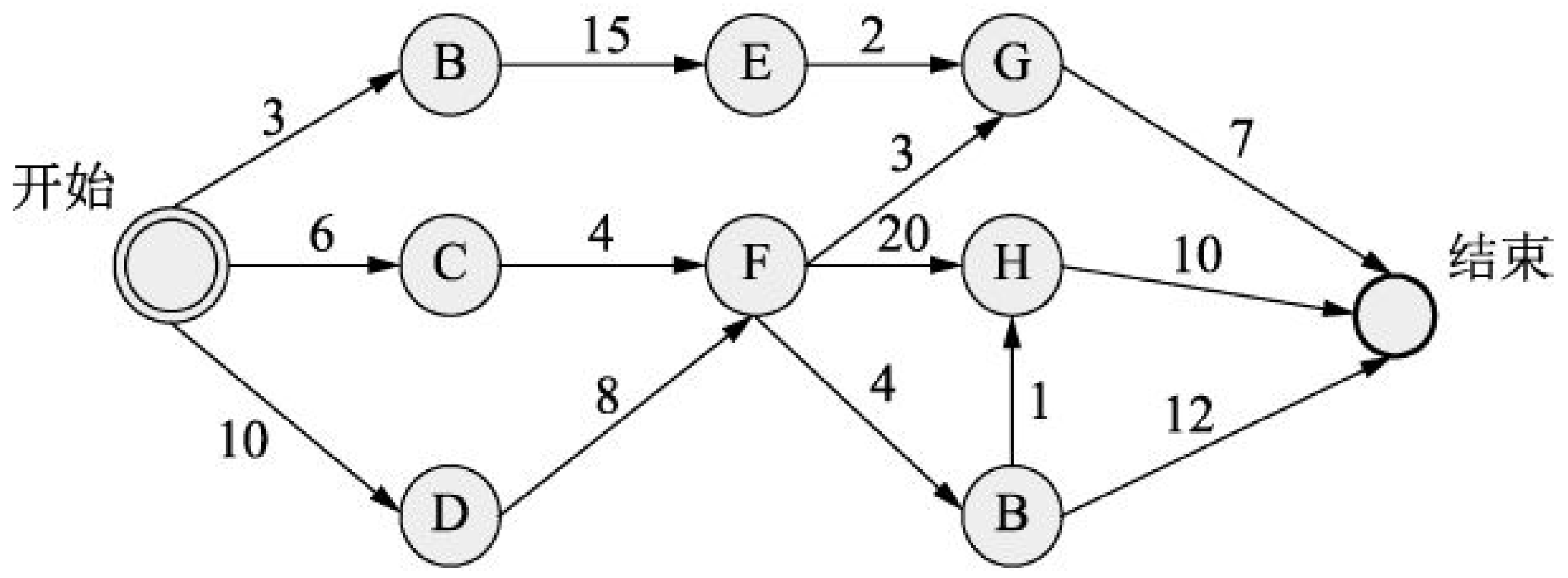
A. 作用范围应该在其控制范围之内

B. 控制范围应该在其作用范围之内

C. 作用范围与控制范围互不包含

D. 作用范围与控制范围不受任何限制

19. 下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，则里程碑__(1)__在关键路径上，活动 FG 的松弛时间为__(2)__。



(1) A. B　　B. C　　C. D　　D. I

(2) A. 19　　B. 20　　C. 21　　D. 24

20. 数据流图(DFD)对系统的功能和功能之间的数据流进行建模，其中顶层数据流图描述了系统的______。

A. 处理过程　　B. 输入与输出　　C. 数据存储　　D. 数据实体

21. 以下关于类继承的说法中，错误的是______。

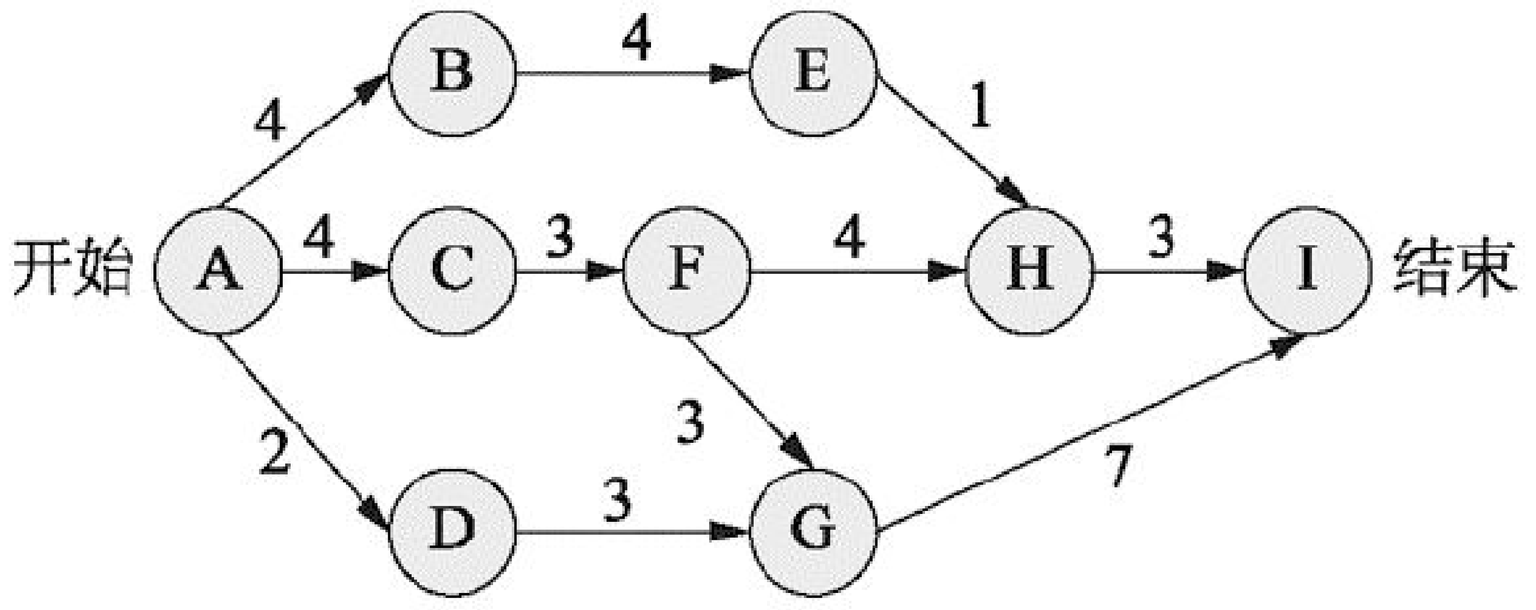
A. 通过类继承，在程序中可以复用基类的代码

B. 在继承类中可以增加新代码

C. 在继承类中不能定义与被继承类(基类)中的方法同名的方法

D. 在继承类中可以覆盖被继承类(基类)中的方法

22. 下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的值表示完成活动所需要的时间，则______在关键路径上。



A. B　　B. C　　C. D　　D. H

23. 软件开发的增量模型________。

A. 最适用于需求被清晰定义的情况

B. 是一种能够快速构造可运行产品的好方法

C. 最适合于大规模团队开发的项目

D. 是一种不适用于商业产品的创新模型

24. 假设某软件公司与客户签订合同开发一个软件系统，系统的功能有较清晰的定义，且客户对交付时间有严格要求，则该系统的开发最适宜采用________。

A. 瀑布模型　　B. 原型模型　　C. V-模型　　D. 螺旋模型

25. 王某是一名软件设计师，按公司规定编写软件文档，并上交文件存档，这些软件文档属于职务作品，且________。

A. 其著作权由公司享有

B. 其著作权由软件设计师享有

C. 除其署名权以外，著作权的其他权利由软件设计师享有

D. 其著作权由公司和软件设计师共同享有

26. M 软件公司的软件产品注册商标为 M，为确保公司在市场竞争中占据优势，对员工进行了保密约束。此情形下该公司不享有________。

A. 商业秘密权　　B. 著作权　　C. 专利权　　D. 商标权

27. 中国企业 M 与美国公司 L 进行技术合作，合同约定 M 使用一项在有效期内的美国专利，但该项美国专利未在中国和其他国家提出申请。对于 M 销售依照该专利生产的产品，以下叙述正确的是________。

A. 在中国销售，M 需要向 L 支付专利许可使用费

B. 返销美国，M 不需要向 L 支付专利许可使用费

C. 在其他国家销售，M 需要向 L 支付专利许可使用费

D. 在中国销售，M 不需要向 L 支付专利许可使用费

13.6.2 参考答案

1. A	2. C	3. D	4. C	5. (1) B (2) C
6. B	7. A	8. B	9. D	10. A
11. D	12. C	13. B	14. C	15. C
16. B	17. (1) C (2) B	18. A	19. (1) C (2) B	20. B
21. C	22. B	23. B	24. A	25. A
26. C	27. D			

第 14 章　计算机专业英语

大纲要求：

- 具有工程师所要求的英语阅读水平。
- 掌握本领域的基本英语词汇。

14.1　计算机网络技术基本词汇

英语词语是最基础的部分。由于网络技术是不断更新的领域，不断有新的思想涌现，也伴随着新的词汇出现。由于新出现的词汇和网络技术的专业性，往往造成理解上的偏差，因此需要应试者在基本了解网络技术中英语专业词汇的基础上，将英语词汇和汉语词汇在功能和语义上相对应，形成正确的理解。

应试者需要准确掌握词语的意义，区分同义词在意义和使用上的差别；准确掌握名词单、复数形式，以及由单、复数形式带来不同语义的解释；准确掌握关系代词、关系副词、联系词在语句乃至整个语篇中的逻辑意义。

在词汇复习中，尤其还需要注意专业词汇的缩写，这些缩写往往是某些技术、设备或协议的代称，在整个试题中是核心词汇。

A

A +　由 CompTIA 创建的，标识关于 PC 操作、修理及管理的专家认证系统。

ACK(应答信号)　在 OSI 模型的传输层中用来通知发送者发送的帧已经收到的应答信号。

active monitor(活动监视器)　在令牌环网络上，负责维护令牌传递、监视令牌和帧的传输、检测丢失的令牌和纠正其他错误的工作站。在任何时候都只能有一个活动监视器。

active topology(动态拓扑)　一种拓扑结构，在这种结构中，任何工作站都参与数据传输。

address(地址)　在网络中唯一标识每个工作站和设备的数字。没有唯一的地址，网络中的计算机就不能可靠地通信。

address management(地址管理)　集中管理整个局域网的地址，通常不需要访问客户工作站。

Address Resolution Protocol(地址解析协议，ARP)　TCP/IP 的一个核心协议。它属于 Internet 层。它得到一个主机或节点的 MAC 地址，然后产生一个本地数据库，把 MAC 地址映射到主机的 IP 地址。

addressing(编址)　赋予网络上每一个工作站设备唯一地址的过程，地址的类型由网络协议和操作系统决定。

AIX(Advanced Interactive eXecutive，高级的交互式执行系统)　由 IBM 实现的 UNIX 系统。

alias(别名)　一个节点主机的别名，可以在一个本地主机文件中指定。

alien crosstalk(外部串扰)　当两根电缆传输时发生的一种相互干扰。

amplitude(幅度)　一种信号强度的表达。

ANSI(美国国家标准化协会)　由来自美国全国工业单位和政府的 1000 多名代表组成，决定电子业以及其他领域如化学、原子能、健康、安全、建筑等的标准的组织。

analog(模拟信号)　用电压的高低产生连续波，进行一种非精确传输的电子信号。

API(Application Programming Interface，应用程序编程接口)　一种允许应用程序与操作系统交互的方法或命令。API 源于 OSI 模型的应用层。

Apache(阿帕奇)　一种流行的、开放源码的 Web 服务器程序，经常用在 Linux 的 Internet 服务器上。

AppleTalk　用来与 Macintosh 计算机互联的协议，虽然 AppleTalk 最初是设计用来支持在 Macintosh 计算机之间进行点对点网络通信的，但它现在也可路由并且可以和 NetWare 和 Microsoft 网络集成。

AppleTalk Network Number(AppleTalk 网络号)　用来标识 AppleTalk 节点上连接的网络的一个唯一的 16 位的数字。

AppleTalk node ID(AppleTalk 节点 ID)　一个用来标识 AppleTalk 网络中的计算机的一个唯一的 8 位或 16 位数字(如果你正在使用扩展网络，在其中一个网络可以有多个地址并支持多个地址)。

AppleTalk Zone(AppleTalk 区)　在 AppleTalk 网络中定义的逻辑组。

application layer(应用层)　OSI 模型的第七层，应用层为要使用网络服务的应用软件提供接口。

application switch(应用交换)　第三层或第四层交换的另一个名称。

array(磁盘组)　一组硬磁盘。

asset management(资产管理)　收集并存放关于一个组织网络中有关软硬件的数量、类型的数据。数据的收集是在一个服务器上自动检测各个工作站而完成的。

asymmetric multiprocessing(非对称多道处理技术)　为指定处理器分配子任务的多道处理技术。

asymmetrical(非对称性)　一种传输技术特性，它表示在一个方向上传输的带宽大于另一个方向。

asymmetrical DSL(非对称性 DSL)　DSL 的一种，当数据下载时比上传时的流量要大。

asynchronous(异步的)　一种传输方法，端与端之间传输和接收时不需要时间上的同步。在异步通信中，一个端子可以在任何时候发送数据而目标端在数据到来时必须接收。

Asynchronous Transfer Mode(ATM，异步传输模式)　1983 年在贝尔实验室提出来的一种技术，但直到 20 世纪 90 年代才被标准化。它依靠定长的数据包使传输速率达到 25～622Mb/s，定长的数据包由 48 字节的数据加 5 字节的头信息组成，定长的数据包允许 ATM 在宽带应用上提供可预测流量的模型和更好的控制。

attenuate(衰减)　当信号从源端传输到较远处时的强度减弱现象。

attenuation(衰减)　在给定距离的信号的衰减量。

authentication(身份验证)　检测一个用户的身份和权限的过程，不同的系统采用不同的验证手段。

autosense(自动检测)　现代网络接口卡的一种特性，它使网络接口卡能自动检测网络上正在运行的帧类型并依据它来完成设置。

B

B channel(B 通道)　在 ISDN 中的“承担”通道，因为它承担点到点的数据流。

backbone(网络主干)　连接每个连接设备或不同层次的连接设备的电缆连接。

backlevelling(恢复版本)　在试图升级一个软件后又恢复到以前版本的过程。

backup(备份)　为安全原因而产生的一个对数据和程序文件的备份。

backup browser(备份浏览器)　一个保持主浏览器浏览列表副本的服务器，在主浏览器失效时可以代替其工作。

Backup Domain Controller(BDC，备份域控制器)　备份主域控制器的账号和安全信息的域服务器。备份域控制器(BDC)也可提供对用户身份的验证。一个域中可以有的备份域控制器(BDC)的数量是没有限制的，但一般至少应该有一个。因为备份域控制器(BDC)必须读写主域控制器(PDC)，所以备份域控制器(BDC)应该在主域控制器(PDC)正常运行后安装。

backup rotation scheme(备份计划)　关于何时和如何备份的计划，决定哪次备份是完全备份、增量备份或差分备份。

bandwidth(带宽)　描述介质所能传输的最高频率与最低频率之间的差值的量。

bandwidth overhead(带宽开销)　为支持可路由协议而在网络基础上的开销。

base I/O port(I/O 端口基址)　一个 16 位设置，决定哪块内存用来作为 CPU 与网络接口卡之间的数据传输通道。像 IRQ(中断号)一样，一个设备的 I/O 端口基址也是不能与其他设备复用的。

baseband(基带)　一种传输模式，数字信号直接把电流脉冲送到电缆线上。这种直接电流传送要求使用电缆的全部基带，所以基带传输只能同时传送一个信号或一个通道。在基带系统中所有设备共享一个通道。

baselining(记录基线)　在网络上测量并记录网络当前状态的操作。

bend radius(弯曲半径)　在保证不引起传输问题的情况下，电缆所能弯曲的最大弧度。在一般情况下，电缆的弯曲半径小于电缆本身半径的 4 倍。

best path(最佳路径)　从网络上一端到另一端的最有效的路径。在系统最优情况下，最佳路径是两点之间的直线路径。

binary(二进制)　用 1 和 0 的编码来表达信息的数制。

binding(绑定)　指定一个网络设备与另一个协同工作的过程。

bio-recognition access system(生物识别访问系统)　通过扫描个人的生理特性(如一个人虹膜的颜色或指纹)来验证用户身份的系统。

BIOS (Basic Input/Output System，基本输入/输出系统)　安装在主板上的系统，用来控制计算机与外围设备之间的通信。

bit(位)　二进制数的单位。一位在二进制编码系统中相当于一个脉冲。它只有两种可能取值：0 或 1。表示信息的长度时，其对应的中文为比特。

blackout(掉电)　电源完全丢失。

block(块)　磁盘空间单位或 NetWare 系统能控制的磁盘空间的最小单位。块越小，需要服务器的内存开销越大。

Block ID(块标识)　MAC 地址的 6 个数字中的第一个，它标识唯一的制造商。

block suballocation(子块定位)　NetWare 的一项技术。它通过使不能占用整数个块的文件只占块的一部分而把其余空间留给其他的数据，从而提高硬盘空间的利用效率。

BNC T connectors (BNC T 形连接头)　在 10Base-2 以太网中用来把节点连接到网络上的连接头。

bonding (绑定)　通过把一个以上 ISDN 通道连接起来而提高吞吐量的过程，如两个 64kb/s 的 B 通道可以连接而产生一个 128kb/s 的通道。

boot sector virus(引导区病毒)　驻留在软盘引导区的一种病毒，它可以感染分区或 DOS 引导区。引导区病毒只有在机器启动时软盘在软驱中才会感染。

Bootstrap Protocol(BOOTP，解包协议) 一种用来简化 IP 地址管理的服务。BOOTP 集中维护一张 IP 地址和它所对应的设备的 MAC 地址的表，当客户机需要时可以分配给客户机。

Border Gateway Protocol(BGP，边界网关协议) Internet 主干的路由协议。Internet 的发展使路由器的负荷不断增加，也促使了 BGP 的发展。BGP 是当前最复杂的路由协议，它的开发者必须考虑在有 100 000 条路径可供选择时如何高效地通过上百个 Internet 主干网。

braiding(锡箔层) 一层锡箔做的薄层，用来屏蔽某些类型的同轴电缆。

BRI(Basic Rate ISDN，基本速率 ISDN) 一种类型的 ISDN，使用两个 64kb/s 的通道和一个 16kb/s 的通道，一般表示为 2B+D。BRI 是家庭用户最常用的 ISDN 类型。

bridge(网桥) 一个很像中继器的设备，它有一个输入口和一个输出口。与中继器不同的是，网桥可以在重新传输之前操作收到的数据。

bridge route(brouter，桥路器) 一种路由器，它可以提供第二层的桥接功能。

broadband(宽带) 一种信息的传输方法，它通过把信号调制到不同频率的射频模拟脉冲来完成。与基带不同的是，宽带传输技术并不使用二进制编码，频分复用技术可以使宽带系统使用多个通道因而传输更多数据。

broadcast(广播) 一种向所有网络上的工作站传输信息的行为。

broadcast domain(广播域) 在虚拟局域网中(VLAN)，必须用第三层设备如路由器和第三层交换机连接，组成第二层网段的端口。

brownout(电压不足) 一种短时间的电压降低现象。一个负荷过载的电路系统会产生这种现象，可以通过灯光变灰暗来识别。

browse list(浏览清单) 所有发布的对浏览器可用资源的列表。

browser(浏览器) 用来发现所有在网络上的共享设备的服务。它还编辑包含所有这些资源的数据库，服务器上也运行浏览器服务。

browser election(浏览器选举) 在所有计算机中决定哪个可以接替主浏览器而保持主浏览器列表的过程。

BSD(Berkeley Software Distribution，伯克利软件版本) 一种由加州大学伯克利分校发布的 UNIX 版本，以 BSD 前缀区别于 AT&T 发布的 UNIX。

bug(故障) 在硬件和软件中引起系统错误的问题。

bus(总线) 在主板上用来在 CPU 和各个部件之间传输数据的电路。大部分奔腾机使用 32 位或 64 位总线交换数据。随着总线位数增加，设备的逻辑也要增加。

bus topology(总线拓扑) 一种网络拓扑结构，所有的设备通过一条电缆连接到网络上。

byte (字节) 8 个数据位的信息。数字系统中，一字节携带一个信息。

C

cable checker(电缆检测系统) 一种简单的手持设备，用来测试电缆是否连接正常。它通常在电缆一端加上电压，然后在另一端进行检测，以确认在另一端是否可以测到电压量。

cable drop(下行电缆) 接入到用户家的一段光纤或同轴电缆。

cable plant(电缆平台) 组成企业范围内的电缆系统的硬件。

cable tester(电缆测试仪) 一种手持设备，不仅可以检查电缆连接，而且也可以确认电缆不超过最大长度，测量电缆的长度、衰减、相近端的串扰、终端电阻、细缆的阻抗等，以通过与失败比率来

表示电线标准，可以保持或打印电缆测试结果。

caching(缓存)　通过把常用的数据保存在物理内存中以备将来使用以提供性能的过程。缓存能加快对服务器的访问，因为操作系统不用到磁盘中去搜索数据。

call tracking system(调用跟踪系统)　用来把问题文档化的程序。流行的如 clientele、Expert Advisor、Professional Help Desk、Demedy 和 Vantive 等。

capacity(容量)　见 throughput。

Carrier Sense Multiple Access with Collision Detection(CSMA/CD)　具有冲突检测的载波监听多路访问共享以太网的通信协议。在 CSMA/CD 中，每个节点在发送前等待一段时间以避免冲突。

Category 1(CAT 1，一类双绞线)　一种类型的双绞线，内含两对线，只适合于发送话音，而不适合于传送数据，它最多只能以 20kb/s 的速率传送数据。

Category 2(CAT 2，二类双绞线)　一种类型的非屏蔽双绞线，内含 4 对线，可以 4Mb/s 的速率传输数据，现代网络已经很少见。

Category 3(CAT 3，三类双绞线)　一种类型的非屏蔽双绞线，可以 10Mb/s 的速率传输数据，带宽可以达到 16MHz。三类线典型运用在 10Mb/s 以太网或 4Mb/s 令牌环网中。网络管理员逐渐用五类线来取代它以获得更高的传输容量。三类线比五类线便宜。

Category 4(CAT 4，四类双绞线)　一种类型的非屏蔽双绞线，内含 4 对线，可以 16Mb/s 的速率传输数据。四类线可以支持 10Mb/s 以太网和 16Mb/s 令牌环网，可以保证 20Mb/s 的传输速率并提供更好的对串扰及衰减的抑制。

Category 5(CAT 5，五类双绞线)　新建网络或升级到高速以太网时最常用的 UTP，内含 4 对线，可以支持 10Mb/s 带宽和 100Mb/s 的传输速率。除高速以太网外，五类线还支持其他高速网络技术，如 ATM、FDDI 等。

Category 6(CAT 6，六类双绞线)　一种类型的非屏蔽双绞线，内含 4 对线，每对都用金属箔屏蔽，整束线又用一层金属箔屏蔽，在第二层屏蔽层之外又加上一层防火塑料层。金属箔屏蔽对串扰影响有良好的抑制作用，所以六类线可以提供 6 倍于标准五类线的吞吐量。

CDFS(CD-ROM File System，光盘文件系统)　用来访问 CD 上资源的只读文件系统。Windows NT 支持这种文件系统，因而可以支持 CR-ROM 的共享。

cell(信元)　一个定长的数据包。在 ATM 技术中，一个块是由 48 字节的数据加上一个 5 字节的块头组成的。

certification(认证)　通过掌握特定的硬件、操作系统、编程语言或软件，并通过考试而得到对其掌握程度的承认过程。

Certified Network Engineer(CNE，认证的网络工程师)　Novell 公司建立的专家认证系统，用来证明一个人对 Novell 网络系统的理解程度。

change management system(变化管理系统)　一种支持个人集中管理网络变化的过程或程序。在小的组织或企业中，变化管理系统非常简单，它可以使个人每次改变网络时都把自己所做的改变添加到一个文档中。在大的组织或企业中，它可能由一个具有图形界面的数据库管理系统组成，根据不同的计算机环境提供不同的内容。

CIR(Committed Information Rate，承诺信息速率)　在租用帧中继线路时保证使用的最小带宽。帧中继的成本部分依赖于承诺信息率。

circuit switching(电路交换) 一种交换类型，在两个网络节点之间传输数据前必须首先建立连接。使用电路的全部带宽，在用户终止两个节点间的通信之前，线路对别的节点是不可用的。

cladding(包层) 包裹在光纤芯层外面的一层玻璃层。包层的作用相当于一面镜子，把到达的光线反射回芯层。这种反射允许光纤在不丢失光信号的前提下弯曲。

client(客户) 在网络中向别的计算机请求资源或服务的计算机。在某些情况下，客户机也可以作为服务器。客户也可指一台工作站的用户。

client redirector(客户机重定向器) 一台客户机在访问服务器时所要求的服务。

coaxial cable(同轴电缆) 一种类型的电缆，由中心的铜线和它外层的金属屏蔽网、再外层的绝缘层组成。是 1980 年为以太网而发展的，在此以后一直是网络的常用介质。

collapsed backbone(易崩溃主干网) 一种企业级的主干网，以交换机或路由器作为多个子网的中心连接点。

collision domain(冲突域) 一组连接的局域网设备，可以引起并检测它们之间的冲突。网桥和交换机可以从逻辑上分开多个冲突域。

command interpreter(命令集成器) 一个(大部分都是基于文本的)程序，能够代替用户输入来执行系统命令或应用程序。通常是执行一系列保存在文件中的系统命令。

communications server (通信服务器) 运行通信服务如 Windows NT 的 RAS 或 NetWare 的 NAS 等的服务器，也叫作访问服务器。

complete trust domain model(完全信任域模型) 一种组织 Windows NT 域的模型，在这种模型中，每个域管理自己的用户、组、账号、文件和打印机。每个域与其他域之间都有一个双向的域委托关系。

Computing Technology Industry Association(CompTIA，计算机技术工业协会) 由计算机制造商、分销商、培训公司等组成的联合体，他们设定工业级的计算机标准。CompTIA 建立并担保 A+和 Network+认证。

conduit(管道) 用来保护电缆的管道，一般用金属做成。

connection-oriented(面向连接) 某些协议的特性，要求在两个节点传输数据之前首先建立一条连接。

connectionless(无连接) 某些协议的特性，允许协议在传输时并不要求事先建立连接。但这样的协议不能保证信息的无错传输。

connectors(连接器) 用来把网络设备连接到电缆的硬件，无论设备是文件服务器、工作站、交换机还是打印机。

container objects(容器对象) 在 NetWare NDS 树中的逻辑子块或分支，用来图形化组织关于位置、部门、功能、安全验证或其他标准事务。

context(上下文) 一种用来在 NDS 树中寻找对象的路由。上下文由一个对象的可组织的单元名构成，从最特殊的到最常用的，加上组织名，相互之间用句号隔开。

contingency planning(防止意外情况计划) 用来确认把偶发错误危及整个工程目标的可能降低到最小的过程。

convergence time(收敛时间) 在遇到路径改变或时间损耗太长时路由器重新寻找一条最佳路径所花费的时间。

core(纤芯) 光纤的中心部件，由一个或多个纯玻璃纤维组成。

core gateways(中心网关) 组成 Internet 骨干网的网关，中心网关由 Internet 管理中心(INC)管理。

cracker (黑客)　利用操作系统或应用程序的知识破坏系统或数据的人。

CRC(Cyclic Redundancy Check，循环冗余校验)　用来验证数据帧中数据准确性的算法。

crosstalk (串扰)　一种由相邻线对之间传输数据而引起的干扰。

CSU(Channel Service Unit，通道服务单元)　一种用 T 载波技术来提供数据终端，提供纠错功能来保证连接完整并进行线路监视的设备。

CSU/DSU(通道服务单元/数据服务单元)　综合提供 CSU 和 DSU 的设备，用来作为 T1 线路在用户端的连接点。

custom installation(自定义安装)　NetWare 提供的安装选项，允许用户决定安装哪些服务或选项。

custom setup(自定义安装)　Windows NT Server 提供的安装选项，允许用户决定安装哪些服务或程序。自定义安装一般比压缩安装花费的时间多。但如果服务器使用特殊的硬件或软件，就必须选择自定义安装。

cut-through mode (切换交换模式)　一种交换模式，交换机在接收整个数据帧之前，先读取帧头信息，决定信息的发送方向。切割交换模式比其他交换模式(如存储和发送模式)速度快，但准确性较差。

Cyclical Redundancy Check(CRC，循环冗余校验)　在以太网帧中使用的算法。CRC 通过计算帧中所有的数据位形成一个 4 字节的值，叫作 FCS，当接收方收到该帧后，通过 CRC 来验证收到的帧与发送时是否相同，如果不同，说明该帧在传输过程中受到损坏，就要求发送方重发。

D

D Channel (D 通道)　在 ISDN 中，D 通道用来传输有关呼叫(如对话初始化或中断信号)、呼叫者身份验证、呼叫传递、参考呼叫等的信息。

daisy-chain(菊花链)　一种设备连接服务。

Data Link Layer(数据链路层)　在 OSI 模型的第二层。数据链路层把网络介质与网络层连接起来。它的主要功能是把从网络层接收来的数据打包成帧，并转换成物理层可以发送的形式。

Data Link Layer address(数据链路层地址)　参见 MAC 地址。

data modulation (数据调制)　用一个信号改变另一个信号的频率、相位或幅度的过程。

data packet (数据包)　从一台计算机发往另一台计算机的信息单元。

dedicated circuits (专用线路)　由通信提供商(如 ISP 或本地电话公司)提供的，两点之间持续的物理的或逻辑的连接。

dedicated service (专线服务)　一种类型数据连接，用户不必拨号到 ISP，连接在任何时候都是可用的。

dedicated line (专线)　一种持续可用的连接，典型的如 ADSL、T1、T3 等。

default gateway(默认网关)　设备要申请子网以外的服务时首先查找的和申请子网内部的服务时最后查找的网关。在邮件服务中，默认网关相当于邮局。

demand priority(事先申请优先级)　100Base-VG 以太网的数据传输方法。在星型或层次网络中，每个要传输的设备发送一个请求给中心集线器，中心集线器只应答一个请求，集线器检查输入数据包，得到目的地址，然后把数据包发送到目的地址。因为事先申请优先级，只有源节点和目的节点可以看见数据。数据从源传送到集线器，然后从集线器传送到目的设备。

denial-of-service attack(停止服务攻击)　对系统的一种攻击方法，用过量的网络流量使系统停止服务。

Device ID(设备 ID 号)　组成设备的 MAC 地址的 6 字节中的第二个，是由生产商加上的。根据设备的型号和生产日期不同而不同。

dial-up(拨号上网) 一种上网的连接方式，在发送端和接收端都使用 Modem，两者之间用 PSTN 或其他线路连接。

dial-up networking(拨号网络) 拨号连接到局域网服务器或 ISP 的过程。也是微软提供的，内含其操作系统中的实现拨号上网的工具软件的名字。

differential backup(差分备份) 一种备份方法，只有上次备份后又改变的部分被备份到存储介质。但不管改变与否，都会标志为已备份。

digital(数字的) 与模拟信号相对，数字信号只由 0 或 1 的脉冲组成。

digital certificate(数字验证) 一个口令保护的加密文件，保存一个人的身份信息，包括公共密钥和私人密钥。公共密钥用来验证发送者的数字签名；私人密钥允许个人登录，管理数字验证系统。

direct infrared transmission(直接红外线传输) 一种类型的红外线传输，要求发送者和接收者都在对方的视野内。

disaster recovery (灾难恢复) 在一个企业级的系统崩溃后，从备份中恢复系统功能和数据的过程。

disk mirroring (磁盘镜像) 一种 RAID 技术，在数据写入磁盘时自动复制到另一个磁盘上。

disk striping (磁盘条带化) RAID 技术的一种简单实现，数据以 64KB 大小的块均匀存储在磁盘组的各个磁盘上。

diskless workstations (无盘工作站) 一种不带硬盘的工作站，依靠一片只读存储器中的信息连接到网上并下载系统文件。

distributed backbone (分布式主干网) 一种类型的企业级的主干网，由许多集线器连接到一系列的中心集线器或路由器上来实现。

domain(域) 通过 Windows NT 操作系统共享账号和安全信息的一组用户、服务器或其他的资源。

domain master browser (域主浏览器) 用来编辑、定位在域内的共享资源的服务器。

domain name (域名) 用来标识一个域的名称，通常域名与公司或其他组织(如大学或军队)相联系。

Domain Name System(DNS，域名系统) 在 20 世纪 80 年代中期发展起来的一套把域名解析为其 IP 地址的系统。DNS 数据库分布在 Internet 上的多个计算机上，以防止因某台计算机崩溃而引起系统崩溃。DNS 是 TCP/IP 服务中属于 OSI 模型的应用层的服务。

dotted decimal notation(点-十进制标识) 代表 IP 地址的一种方法。为了使 IP 地址更易识别，用十进制的 1～255 代表一个字节的二进制数，相互之间用点隔开。

downstream (下传) 把本地 POP 邮箱内的内容传给用户。在非对称通信过程中，下传的带宽通常比上传的大很多；而在对称通信中，两者带宽相同。

DSL(Digital Subscriber Lines，数字预定线路) 远程的或广域网连接的专用线路，使用先进的数字调制技术在普通的电话线上得到更大的带宽，常用的为非对称的 DSL(ADSL)。

DSU(Data Service Unit，数据服务单元) 一种使用 T 载波技术的设备，用来把网桥、路由器及多路器使用的数字信号转换成可在线路上传输的信号。一般 DSU 和 CSU 放在一个盒中，叫作 CSU/DSU。

Dynamic Host Configuration Protocol(DHCP，动态主机配置协议) TCP/IP 在应用层的一个服务，用来在网络上动态分配 IP 地址，利用 DHCP 可以最大限度地减少 IP 地址冲突的可能性。

E

e-commerce (电子商务) 一种在 Web 上进行商业活动的方法。不管是零售业、银行业、股票交易、咨询或培训，所有在 Internet 上进行的买卖或服务都属于电子商务。

echo reply (应答) 在一个设备 ping 另一个设备时，目标设备的应答信号。

echo request (应答要求) 在网络上一个设备 ping 另一个设备时要求目标设备做出应答。

EIA (Electronics Industry Alliance，电子工业联盟) 一个由来自美国的电子厂家的代表组成的联盟。

ElectroMagnetic Interference (EMI，电磁干扰) 一种由诸如马达、电力线、电视、复印机、日光灯或其他此类电子设备产生的干扰。

emergency repair disk (紧急修复盘) 一张用来在 Windows NT 崩溃后，恢复以前软件和硬件设置的软盘。它可以恢复丢失的或损坏的系统文件和注册表，在安装操作系统时应该做出这张盘。

encrypted virus (加密病毒) 一种病毒，用自身加密的办法来避过检查。

encryption (加密) 利用算法来打乱数据，只有用解密算法才能得到最初的数据，从而实现信息保密。最流行的加密算法是在原数据的每个字节加入一个或多个密钥，从而产生加密的数据块。

enhanced CAT5(增强型五类线) 一种更高级的五类线，内含高质量的铜芯，并且具有更高的扭绞率，另外，还使用其他的先进方法来减少串扰。增强型五类线可以支持 200Mb/s 的传输速率，是标准五类线的两倍。

Enhanced Interior Gateway Routing Protocol(EIGRP，增强的内部网关路由协议) 增强的内部网关路由协议是由 Cisco 公司在 20 世纪 80 年代中期开发的路由协议，它比 OSPF 速度快、开销低、容易配置。EIGRP 还能够支持多种协议，可以减少路由器之间不必要的网络流量。

enterprise (企业) 一个组织的全部，包括当地或远程办公室、不同的计算环境、许多部门等。企业级的计算应该考虑一个大组织的计算环境的广度和差异性。

erasable programmable read-only memory (EPROM) 可擦除可编程只读存储器。电路板上的一种元件，它内部的信息可以被擦除、重写。例如，可以通过改写网络接口卡上的 EPROM 来改变其默认设置。

Ethernet (以太网) 1970 年由 Xerox 公司发展起来，后经 DEC、Intel、Xerox 公司改进的一种网络技术。如今，有 4 种以太网技术，由 IEEE 标准分别设定。

Ethernet 802.2 (802.2 以太网) Novell 公司的 NetWare 操作系统设定的默认的帧类型，它支持 IPX/SPX 协议，在逻辑链路层(数据链路层的一个子层)定义数据的特征，如源、目的等。

Ethernet 802.3 (802.3 以太网) 最初的 NetWare 网帧类型，也是 NetWare 3.12 以下版本的默认帧类型，它支持 IPX/SPX 协议。Ethernet 802.3 有时也叫作“粗 802.3”，因为它只含数据而不包含控制信息，像未加工的原材料一样。

Ethernet II(II 型以太网) 最初由 Xerox、DEC、Intel 公司共同发展的一种以太网类型，II 型以太网没有逻辑链路层信息，代之以一个两字节的标识上层协议的字段。

Ethernet SNAP 802.2 以太网和 II 型以太网的一种融合。SNAP 代表子网访问协议。在帧的 SNAP 块包含 3 个逻辑链路层字段(DSAP、SSAP 和控制信息)，另加上一个字段：组织 ID，用来标识帧运行的网络类型。另外，SNAP 以太网与 II 型以太网一样携带以太网的类型信息。

express setup (压缩安装) 安装 Windows NT Server 的一种选项，只选中那些最常用的选项。压缩安装比自定义安装要快。

extended attributes (扩展属性) HPFS 除支持基本的读、写和隐藏属性以外，还支持扩展属性。

Extended Industry Standard Architecture (EISA，扩展工业总线) 一种与旧的 ISA 总线兼容的 32 位总线，使用一个更深的插槽以提高数据吞吐率。EISA 总线是在 20 世纪 80 年代后期开发出来的，用来替代 IBM 的 MCA 总线。

extended network prefix (扩展网络前缀) 网络地址和子网信息的联合。通过使用扩展网络前缀，一个设备可以确定一个地址属于哪个子网。

F

fail-over(失败接替) 一个元件(如网络接口卡或服务器)在没有人工干预的情况下，在另一个元件失败时自动代替它工作。

failure(失败) 在一段时间内，在一定水平层次上与系统性能的偏离。失败在一些部件没有按预期正常工作时发生。

Fast Ethernet (快速以太网) 参见 100Base-T。

FAT(File Allocation Table，文件分配表) 20 世纪 70 年代发展起来的最初的微机文件系统，支持软盘和后来的硬盘。FAT 对大部分的服务器操作系统来说都是不足的。

FAT32 加强型的 FAT，它在一个磁盘上实现了长文件名和更小的分配单元。FAT32 比 FAT 有更高的磁盘利用率。

fault (错误) 系统中的一个设备不能正常工作，一个错误可能导致系统失败。

fault tolerance (容错) 一个系统在遇到硬件或软件故障时仍能正常工作的能力。

FDDI(Fiber Distributed Data Interface，分布式光纤数据接口) 20 世纪 80 年代中期由 ANSI 定义后又被 ISO 重新定义的网络标准。FDDI 使用光纤以 100Mb/s 的速率传输数据，80 年代和 90 年代早期一般用于主干网，快速以太网技术在 20 世纪 90 年代提出后已逐渐退出市场。FDDI 有良好的安全性和可靠性。

feasibility study (可行性研究) 对一个工程的成本、利润进行研究，并试图预测工程能否带来有价值的产出(如工程能否在不给公司造成沉重的资本和时间负担的前提下达到最初的目标)的过程。

fiber-optic cable (光纤电缆) 一种类型的线缆，内含一股或几股光纤，数据通过激光或发光二极管产生的光脉冲在内层进行传输；外层是包裹的一层玻璃，像镜子一样，根据不同的传输模式，以不同的方式把内层到达的光反射回内层；在包裹层的外面，有一层塑料层和 Kevlar 网来保护芯层；最外面有一层塑料包裹。

file-infected virus (文件型病毒) 一种病毒，它把自己附加在可执行程序文件中，当被感染的文件调入内存时，它把自己复制并附加在别的运行文件中。

file-server (文件服务器) 一台运行网络操作系统的计算机，它使连在网络上的工作站都能共享它上面的资源。

file services (文件服务) 文件服务器的功能，允许用户共享文件、应用程序和存储区。

file system (文件系统) 操作系统用来组织、管理、访问文件的方法，通过逻辑结构和软件方法来实现。

File Transfer Protocol (FTP，文件传输协议) 一个应用层的 TCP/IP，用来管理 TCP/IP 主机间的文件传输。

filtering database (过滤数据库) 由网桥产生和使用的数据表，它包含 MAC 地址和与其相连的工作站的位置信息，也叫作桥接表。

firewall(防火墙) 一种特殊设备(一般为一个路由器，也可能是一台运行特殊软件的 PC)，它有选择地过滤或分配网络间的通信量。防火墙可以是硬件的，也可以是硬件和软件混合的。

firmware (固件) 硬件和软件的结合。固件的硬件部分是一块只读存储器(ROM)，内含出厂时写入的、

可以被设置程序修改的数据。

flavor(风格)　用来说明不同类型的 UNIX 类操作系统的名词，如 Linux 的不同风格包括 Red Hat、Caldera 和 Slackware。

flow control(流控制)　根据接收方的接收速度来控制数据的传输方法。

forwarding table　参见 filtering database(过滤数据库)。

fractional T1(分割 T1 线路)　一种允许多个单位使用一条 T1 线路中的不同通道，从而只为所使用的通道付费的方法。

frame (帧)　一种数据包，它不仅包含原始数据，同时也包含发送者和接收者的地址及控制信息。

Frame Check Sequence(FCS，帧校验序列)　在一个帧中负责数据的无损伤传输的字段，它使用诸如 CRC 类的算法来验证数据传输的完整性。

frame relay (帧中继)　一种升级的、数字版本的 X.25，它是基于数据包交换的。因为帧中继是数字传输，它最大可支持 1.544Mb/s 的传输速率，大于 X.25 的带宽。它是提供许多 Internet 连接的基础。在网络结构中，帧中继经常被描述为云状。

FreeBSD　一种开放源码的伯克利版的 UNIX。

freely distributable(自由发放)　一个用来描述软件具有非常自由的版权的名词，经常伴随着开放源码。

frequency(频率)　信号幅度在一个给定时间内的变化次数，通常用每秒的周期数来表达，单位为 Hertz(Hz)。

full backup (完全备份)　一种备份方法。服务器上的所有数据，不管是新的还是未改变的，都备份到存储介质上。

full duplexing (全双工)　在网络的两个节点之间，在没有冲突的情况下允许双向传输。全双工可以使网络的带宽加倍。

full synchronization(完全同步)　一个把主域控制器(PDC)上的用户账号数据库完全复制到备份域控制器(BDC)上的过程。管理员可以强制进行完全同步，但它可能产生过多的网络流量。

fully qualified host name (完整的主机名)　一个主机的名称，不仅包含主机名，而且包含其所在的域。如 mymachine.domain.org。

G

Gantt chart (甘特图)　一种流行的、通过一个水平的时间来描述工程开始到结束的信息的方法。

gateway (网关)　一个硬件和软件的结合，它连接不同类型的网络。网关提供连接、会话管理和数据翻译，所以它们在 OSI 模型的所有层工作。

Gateway Services for NetWare (GSNW，NetWare 网关服务)　Windows NT 提供的一个服务，用来充当 Windows NT 和 NetWare 客户重定向器之间的翻译。通过安装 GSNW，Windows NT Server 可以访问 NetWare 服务器上的文件和其他资源。

ghosts (畸变帧)　并非真的数据帧，而是由于中继器译错的寄生电压引起的失真。与真正的数据帧不同，畸变帧没有起始位。

giants (巨型帧)　超过介质允许的最大值的数据帧。例如，超过 1518B 的以太网帧就可以称为巨型帧。

global group (全局组)　一组属于多个域的用户或资源。

globbing　文件名的一种替代形式，与 Windows 和 DOS 使用的通配符类似。

GNU(Gnu’s Not UNIX)　用完全开放源码实现 UNIX 的自由软件工程的名字，应用程序和工具包含在

Linux 和其他自由软件 UNIX 系统中，可重复的词头代表 GNU 而不是 Linux。

gopher 一种基于文本的应用程序，允许通过一系列的菜单找到并阅读文件。

grandfather-father-son 一种备份循环计划，使用天、周、月备份来设置。

graphical user interface (GUI，图形用户接口) 一种基于图形的计算机功能或模块。在网络操作系统中，可以使管理员更容易地管理文件、用户、组、安全、打印机及此类问题。

group(组) 用来集中管理用户对于资源的权限的一种方法。组是任何类型的网络操作系统管理资源和用户的基础。许多管理员根据部门或同一部门内不同的工作性质建立组。

H

hacker(黑客) 掌握操作系统内核的工作机理，并用此来尝试进一步理解操作系统的人。

hard disk redundancy (硬磁盘冗余) 参见廉价磁盘冗余阵列。

Hardware Compatibility List (HCL，硬件兼容列表) 已经测试过可以在 Windows NT Server 下正常运行的硬件列表。包含在 Windows NT Server 的安装 CD 中，也可以在微软的网站上找到。

head-end 电缆公司的中心办公室。在到达用户之前，它连接了许多节点。

Hertz (Hz，赫兹) 频率的度量单位，等于每秒振幅循环的次数。

heuristic scanning (渐进式扫描) 一种类型的病毒扫描，试图通过“病毒式的”行为来鉴别病毒。

hierarchical file system (层级文件系统) 在一个磁盘分区上文件和目录(文件夹)的组织形式，其中目录可以包含文件和子目录。如果在图形方式下展开，整个组织像一棵树。

hierarchical hybrid topology (树型混合拓扑) 一种网络拓扑结构，根据设备的功能或优先级，用层来隔离设备。

host (主机) 一台用 TCP/IP 连接到网络的计算机。

host file (主机文件) 一个文本文件，内含 TCP/IP 主机名与其 IP 地址的信息。在 Windows 95 和 Windows NT 平台上，此文件叫作 imhosts。

host name (主机名) 用来描述 TCP/IP 设备的符号名。

hot swappable (可热交换的) 设备的一种特性，允许当设备产生错误时自动用其副本来代替。

HOWTO (操作指导) 一系列简短的、高度集中的文档，给出 Linux 系统的细节，负责 Linux 工程文档的人集中管理这些文档。

HP-UX 惠普公司的 UNIX。

HPFS (High-Performance File System，高效文件系统) 一种为 OS/2 系统设计的文件系统，它比 FAT 系统有更高的效率和可靠性。现在已经很少使用，但 Windows NT 支持 HPFS。

hub(集线器) 一个多端口的中继器，其中一个端口用来连接主干网，其余的端口用来连接一组工作站。集线器可以再生信号。

Hybrid Fiber-Coax (HFC，混合光纤—同轴电缆) 一种由光纤和同轴电缆组成的连接，由光纤从办公室连接到用户附近的节点，然后用同轴电缆连接到用户。在有线电视电缆可以用作广域网连接以前，HFC 必须升级现有的电缆。

hybrid topology (混合拓扑) 一种由简单的拓扑连接成的复杂的拓扑结构。

Hypertext Transport Protocol (HTTP，超文本传输协议) Web 客户端和服务器之间的通信语言。HTTP 组成了 Web 的骨干。

I

i-node (i-节点)　一个 UNIX 文件系统信息存储区。存储信息包括文件大小、访问权限、产生时间和一个指向该文件内容的指针。

IEEE (Institute of Electrical and Electronic Engineers，电子电气工程师协会)　一个由工程专家组成的国际组织。它的目标是提高电子和计算机领域的发展和培训水平。

incremental backup(增量备份)　一种备份方法，只有在上次备份后改变的部分才进行备份。

indirect infrared transmission(间接红外线传输)　一种类型的红外线传输方法，信号通过墙壁、屋顶和其他物体反射，因为间接红外线信号传输没有一个事先限定的路线，所以传输的可靠性不高。

Industry Standard Architecture(ISA，工业标准总线)　最初的 PC 总线，20 世纪 80 年代初期发展用来支持 8 位以及后来的 16 位数据传输。尽管是较古老的技术，ISA 总线现在仍用来连接一些串行设备，如 Modem 和 Mice。

infrared(红外线)　一种类型的数据传输，使用红外线作为传输介质，像远程电视发射那样进行传输。网络中使用两种类型的红外线传输：直接红外线传输和间接红外线传输。

integrity (完整性)　网络文件、系统和连接的统称。为了保证完整性，必须保护网络系统免受诸如崩溃、随意窜改、自然灾难和病毒的破坏。

integrity checking (完整性检查)　一种用现有的文件和磁盘与已归档的版本相比较而发现差异的方法。最经常的完整性检查包括检查数目。

intelligent Hub(智能型 Hub)　一种类型的集线器，不只具有简单的再生信号的功能，而且可以在每个瞬间通过指定哪些节点有发送和接收权限来管理数据传输。

Internet　一个复杂的连接全球的局域网的广域网。

Internet Control Message Protocol(ICMP，Internet 控制消息协议)　TCP/IP 的核心协议之一，用来通知发送方数据在传送过程中出错。

Internet Mail Access Protocol(IMAP，Internet 邮件访问协议)　依靠 SMTP 传输系统的邮件存储和管理协议，可以改进 POP 的缺点。最流行的是版本 4(IMAP 4)，IMAP 4 最终将取代 POP，而用户不必更换 E-mail 软件。与 POP 相比，IMAP 4 最大的优点是，用户可以在邮件服务器上存储消息而不必总是必须把它们下载到本地。

Internet Protocol(IP，网际协议)　TCP/IP 的核心协议之一，属于 TCP/IP 的 Internet 层，提供数据传输的目的和方式。IP 是使 TCP/IP 可以工作在网间的子协议。

Internet services(Internet 服务)　使网络能够与 Internet 通信的服务，包括 Web 服务器和浏览器、文件传输程序、地址解析、安全过滤和一种直接登录到其他计算机的方法。

Internet telephony (Internet 电话)　在 Internet 上提供的电话服务。

Internetwork(网络互联)　网络产品和服务供应商网络产品和服务的术语，是一个允许人们和他们的计算机通过不同类型的网络通信的所有概念、技术和普通设备的通用术语。

Internetwork Packet eXchange(IPX，网间网数据包交换)　IPX/SPX 的核心协议，在 OSI 的网络层操作，提供路由或网间服务，与 TCP/IP 中的 IP 功能类似。

Internetwork Packet eXchange/Sequenced Packet eXchange(IPX/SPX)　最初由 Xerox 公司开发出来的网络协议。20 世纪 80 年代，Novell 公司采纳并修改了 IPX/SPX，用在 NetWare 网络操作系统中。

InterNIC　负责 IP 地址分配和域名注册的权威机构，也叫作 Network solutions。

intraNetWare Net Ware 4.11 的另一个名称，也是最早支持 Internet 服务的版本。

intrusion detection(侵入监视) 监视网络防止非授权访问的过程。

IP address (IP 地址) TCP/IP 联网中使用的逻辑地址，由一个分成 4 组，相互之间用点隔开的 32 位数构成。

IP datagram (IP 数据报) TCP/IP 帧中的 IP 部分像一个包含数据的信封，保存路由器在不同子网间传输帧的必要信息。

IP Security protocol (IPSec，IP 安全协议) 一个属于新版的 TCP/IP IPv6 的第三层协议，定义加密、验证和密钥管理。IPSec 为每个 IP 数据头加上安全信息。

IP spoofing (IP 电子欺骗) 一种安全攻击，网络以外的用户得到内部的 IP 地址，然后用此 IP 地址假装他或她具有访问内部网的权限。

IPX address (IPX 地址) 在 IPX/SPX 协议中对一个设备指定的地址。

IRQ (Interrupt Request Line，中断请求线) 设备请求 CPU 服务的方法。IRQ 由 0～15 标识。许多 PC 设备保留特殊的 IRQ 并独占它。

ISDN (Integrated Services Digital Network，综合业务数字网) 一种由 ITU 建议的，用来通过数字线路传输数据的国际标准。与 PSTN 一样，ISDN 使用电话载波线路和拨号连接；但与 PSTN 不同，ISDN 使用数字线路和交换设备。

ISO(International Organization for Standardization，国际标准化组织) 代表 130 个国家的标准化组织的联合，总部设在瑞士日内瓦。它的目标是实现国际的技术标准，实现全球信息交换和无壁垒贸易。

ITU(International Telecommunications Union，国际电信联盟) 一个联合国组织，规范国际电信，包括电台和电视频段、卫星和电话技术、网络结构和全球通信税率。它也向发展中国家提供技术和设备，用来改善这些国家的技术基础。

J

jabber(故障点) 一个处理不正常电信号的设备，该信号通常会影响网络的其余部分。网络监视器会发现有一个设备总在重复发送数据，从而使网络停止工作。通常情况下是由坏的网络接口卡引起的，偶尔也会因为外界电磁干扰造成。

jamming (阻塞) 一个工作站的网络接口卡首先广播一个冲突，其他工作站停止发送，在广播冲突后，网络接口卡在一段时间内不再发送。

K

kernel (内核) 一个操作系统的核心， NetWare 的 32 位内核负责监视所有的服务器进程。SERVER EXE 程序从服务器的 DOS 分区运行内核。

kernel modules (内核模块) Linux 的内核部分，可以加载或卸载，也可以加上或去除正在运行的 Linux 系统内核的某些功能。

key(密钥) 一系列字符，在许多加密算法中用来使解密更困难。

L

LAN topology (局域网拓扑结构) 一个局域网的物理设计。

LAN analyzer(局域网分析器) Novell 公司的网络监视软件包。LAN analyzer 可以在 Windows 95 或 Windows 98 中当作一个单独程序，也可以作为 NetWare 服务器上的网络管理工具 Manage Wise

的一部分。LAN analyzer 提供以下功能：发现网段上的所有节点，持续监视网络流量，在网络传输达到一个预设值时报警(比如带宽占用超过 70%)。捕捉目的或源地址为所有节点的帧。

late collisions(不可探测的冲突)　冲突发生在可被探测并纠正的范围外，通常是由一个故障工作站(如一个网络接口卡、收发器等)在验证线路状态以前发送数据或通过失败观察电缆长度的配置指南，这将导致冲突被识别得太晚。

latency (持续时间)　信号传输到它被接收之间的延时。

layer (层)　在网络上对不同设备的逻辑划分。

Layer 2 Forwarding(L2F，第二层发送)　在第二层的与 PPTP 相似的协议，它为其他协议提供管道，能和 PPP 使用的验证方法协同工作。L2F 是由 Cisco 公司开发的，要求在主机系统端有特殊的硬件。与 PPTP 不同，它可以封装协议以适合 IP 以外的格式。

Layer 2 Tunneling Protocol (L2TP,第二层隧道协议)　由许多工厂合作开发的第二层隧道协议，是 L2F 的增强型版本，它不要求昂贵的硬件设备。L2TP 为下一代 IP(IPv6)和 IPSec(第三层加密协议)作了优化。

Layer 3 switch (第三层交换)　能够在 OSI 的第三层(网络层)操作数据的交换机。

Layer 4 switch (第四层交换)　能够在 OSI 的第四层(传输层)操作数据的交换机。

leaf object (叶对象)　一种类型的 NDS 对象，它不包含其他对象。例如，一个打印队列是一个叶对象，因为它只操作打印队列。

lease (租用)　DHCP 服务器和客户端使用 DHCP 分配的 IP 地址的时间长度的协议。作为管理员，可以根据需要设置相同时间，从几分钟到永远。

leased lines (租用线路)　通过公用的通信载体建立的永久的专用连接，用户按月付租金。

license tracking (许可跟踪)　检测网络中正在使用的单个应用程序的副本数。

line noise (线路噪声)　由网上的其他设备引起的或由电磁干扰引起的电平的涨落。

Linux　一个自由分发的 UNIX 版本，最初是由芬兰计算机科学家 Linus Torvalds 完成的。

load balancing(负载平衡)　自动地把数据流量分配到多个链接、硬盘或处理器，从而优化响应时间。

Local Area Network (LAN，局域网)　由分布在一个相对较小区域的计算机和其他设备组成的网络，如在一栋大楼甚至在一个办公室。

local collisions (本地冲突)　当两个或多个工作站同时发送数据时产生的冲突，当冲突率很高时往往是电缆或路由的问题。

local computer (本地计算机)　一组属于同一个域的用户或资源。

local loop (本地环)　连接用户与公共载波 POP 的电话系统。有些广域网连接方法，如 ISDN，只适合作为网络连接的本地环部分。

Logical Link Control (LLC) sublayer(逻辑链路子层)　数据链路层中的上子层。逻辑链路子层提供了一个公共接口，并提供可靠性和流控制服务。

logical topology (逻辑拓扑)　网络设计的数据传输特征，如网络传输模型。

loopback address (回送地址)　一个 IP 地址，用作从一个节点到它自己的通信(通常为了检测目的)。本地循环地址总是 127.0.0.1。

loopback plug (回送连接插头)　用来排除故障的插头。把它插入一个端口(如串口或并口)，然后交叉连接传输线和接收线，允许信号传回计算机来检测。

M

MAC address (MAC 地址)　一个唯一标识网络节点的数字。制造商把 MAC 地址写入网络接口卡中。MAC 地址是由块 ID 和设备 ID 构成的。

macro viruses (宏病毒)　一种采用 Word 或 Excel 中宏形式的新病毒，它可以在 Word 或 Excel 使用时被执行。

mail services (邮件服务)　在用户和网络之间管理存储和传输 E-mail 的网络服务。除了发送、接收和存储邮件以外，邮件服务还可以为其他邮件服务器提供智能 E-mail 路由能力，提供通知、计划、附件、文档库和网关等服务。

managed Hub (可管理 Hub)　参考 Intelligent Hub(智能集线器)。

management services (管理服务)　在网络上用来集中管理并简化复杂的管理任务的网络服务，如许可追踪、安全审查、资产管理、地址分配、软件发布、流量检测、负载平衡和硬件诊断等。

manual pages (手册)　UNIX 的在线文档，描述 UNIX 命令及程序接口的使用。

master browser (主浏览器)　在一个网络中定位共享资源并维护一个此类信息的数据库的服务器。默认的主域控制器(PDC)作为一个域的主浏览器。

master domain model (主域模型)　一个组织 Windows NT 域的方法，其中一个域管理所有的用户账号信息，而其他的域管理网络资源如打印机等。这个模型适合于企业的每个部门管理自己的文档和打印机，而一个中心的技术信息部门管理所有的用户、组以及域之间关系的环境。

Media Access Control (MAC) sublayer (MAC 子层)　数据链路层中的下子层。MAC 子层把目的计算机的物理地址附加在帧的后面。

megabits per second (Mb/s，兆字节每秒)　网络传输速度的单位，通常与网络的物理特征有关。

member server (MS，成员服务器)　在 Windows NT 域中，不负责管理用户账号和安全信息的服务器。一个成员服务器通常是专门用来运行一个需要专门的处理器资源的应用程序，如 MS SQL Server。

memory range (内存区)　一个十六进制数，用来指明网络接口卡和 CPU 交换数据所用的内存区域。与 IRQ 一样，某些内存区是为某些特殊设备预留的。常见的如主板。

mesh network (网状网络)　一个企业级的网络拓扑，其中路由器与其他多个路由器相连，所以在任何两个节点之间至少有两条路由。

mesh WAN topology (网状广域网拓扑)　一种广域网技术，由许多直接相连的节点组成复杂的网状网络。

message switching (消息交换)　一种交换方式。首先在两个设备之间建立连接，一个设备发送数据到第二个设备，然后断开连接。第二个设备保存数据直到与第三个设备建立连接，然后把数据发送给第三个设备。重复这样的过程直到数据到达目的地。

MIB (Management Information Base，管理信息库)　由管理程序收集的一组数据，用来分析网络性能或问题。管理程序可以是网络操作系统的一部分或是第三方的程序。

Micro Channel Architecture (MCA，微通道总线)　IBM 的个人计算机的 32 位总线，1987 年引入，后来被 EISA 和 PCI 代替。

Microsoft Certified Systems Engineer (MCSE，微软认证的系统工程师)　微软公司建立的专家认证系统，用来证明一个人对微软产品，包括 Windows NT 和 Windows 98 的掌握程度。

Microsoft Message Queueing (MSMQ，微软消息队列)　在网络环境下使用的一个 API，MSMQ 把在

节点之间传输的消息保存在一个队列中，当与目的节点的连接可用时才发送这些信息。

milestone (里程碑) 标明一个工程中的任务或任务组完成的标志，用来衡量工程的进展情况。

modem (调制解调器) 在发送端把数字信号调制得到模拟信号以便通过电话线传输，而在接收端把信号解调得到数字信号的设备。

modular Hub (模块式集线器) 一种在底盘上提供多个接口的集线器。与 PC 一样，模块式集线器有一个主板，主板上有为不同适配卡预留的插槽，这些适配卡可以连接到不同类型的集线器、路由器、广域网，还可以连接到令牌环和以太网的主干网。它们也可以连接到插件式集线器来管理工作站或冗余器件，如附加电源。

modular router (模块式路由器) 具有多个插槽的路由器，通过使用不同的接口卡或其他设备来提供可选的、可靠的网络间操作能力。

monitor(监视器) 一个 NLM，通过一系列菜单可以设置网络接口卡、协议绑定顺序、安全性、连接和其他许多服务器参数。

multimode fiber (多模光纤) 一种可在其内同时传送几种波长的光的光纤，常用在数据网中。多模光纤比单模光纤便宜。

multiple master domain model (多主域模型) 一种组织 Windows NT 域的方法，其中两个或多个主域通过建立双向委托关系来管理许多资源域。

multiplexer (多路复用器) 把一个通道划分为多个，用来传输语言、数据或其他信号。

multiprocessing (多道处理) 把任务在多个处理器间分隔以加速指令执行的技术。

multiprotocol network (多协议网络) 使用一个以上协议的网络。

Multistation Access Unite (MAU，多路访问单元) 在令牌环网中使用的设备，能够中继信号，与集线器功能相当。

N

name server (命名服务器) 一个包含 TCP/IP 主机名和它们关联的 IP 地址的数据库的服务器。命名服务器提供命名解析服务，当它不能解析 IP 地址时，它把查询转到上一级的服务器。

name space (命名空间) 包含 Internet 上的 IP 地址和它们对应的主机名，以及分布在全球 DNS 命名服务器上的数据库。

narrowband (窄带) 一种类型的发射频率，信号以一个单一频率传送。电台和电视使用这样的方法，因为信号容易被接收和解码。

Nbtstat 一个 TCP/IP 中用来查错的工具。提供 NetBIOS 名与它对应的 IP 地址的信息。如果知道一个工作站的 NetBIOS 名，就可以使用它的 Nbtstat，得到它的 IP 地址。

NDS for NT Novell 公司的 Windows NT 域在 NWAdmin 中以一个客户对象出现。

NDS tree (NDS 树) 在企业环境下，NetWare 把资源分组的逻辑表示。

needs assessment (需求评估) 协议中的改进原因和目标，从而判断它是否值得或必要，从而说明改进的细节。

negative frame sequence checks (帧校验序列错) 接收端计算的 CRC 值和发送端的 CRC 值不匹配。它通常是由于局域网内的噪声和传输接口的问题，也可能是电缆原因造成的，如果出现的频率较高，说明网上有太多的冲突或其中有工作站持续发坏帧。

NetBEUI (NetBIOS Enhanced User Interface，增强型 NetBIOS 用户接口) 微软公司实现的与 IBM

NetBIOS 协议兼容的协议，NetBEUI 通过添加一个应用层组件而扩展 NetBIOS，NetBEUI 是一个快速、高效而且占用很少资源的协议。提供优秀的纠错功能，几乎不要求手工配置。

Netstat 一个 TCP/IP 中用来查错的工具。它显示当前 TCP/IP 连接的信息，它也显示端口号，可以通过它查看服务是否使用了正确的端口。

NetWare 3.x 一组 NetWare 版本，包括 3.0、3.1、3.2。

NetWare 4.x 一组 NetWare 版本，包括 4.0、4.1、4.2。

NetWare Administrator utility (NWAdmin) NetWare 图形化管理工具，允许管理员从 Windows 95、Windows 98 和 Windows NT Workstation 下来管理 NDS 树。

NetWare Core Protocol (NCP，NetWare 核心协议) 一个 IPX/SPX 协议的核心协议，处理客户机和服务器之间的服务请求，如文件访问或打印。

NetWare Directory Services (NDS，NetWare 目录服务) 管理多个服务器和它们资源的系统，包括用户、卷、组、登录界面和打印机。NDS 模型与 NT 下的域模型类似，但更容易理解。在 NDS 中，每个网络资源都被当作单独的具有特定属性的对象来对待。

NetWare Loadable Modules (NLMs，NetWare 可加载模块) 使服务器能够运行程序和服务的方法。每个 NLM 占用服务器的一部分内存和处理资源，NetWare 的核心允许同时运行许多 NLM。

network (网络) 通过某种传输介质(通常是线或电缆)连接起来的一组计算机或其他设备(如打印机)。

Network+(Net+) CompTIA 建立的专家认证系统，认证很大范围内的网络技术，如对协议、拓扑结构、网络硬件和网络查错的理解。

network analyzer(网络分析仪) 手持的基于硬件的工具。可以连接到网络上来解决问题。通常工作在 OSI 模型的第七层。

network architect (网络架构师) 一个专业工作者，完成网络设计任务，从选择基本器件(如电缆类型)到正确设置，使这些组件正常工作(如选择正确的协议)。

Network Interface Card(NIC，网络接口卡) 使一个工作站连接到网络并能与其他计算机通信的设备。网络接口卡可由几个不同的公司制造。可根据工作站和网络的要求，有一系列设置。

network layer (网络层) OSI 模型的第三层。网络层把网络地址翻译成物理地址，并解决从发送者到接收者的路由问题。

network layer addresses(网络层地址) 在 OSI 模型的网络层驻留的地址，可以构成有一个树状地址表，并可以通过操作系统工具设置。

network monitor (网络监视器) 一种软件工具，可以持续监测从一个服务器或工作站来的网络流量。网络监视器通常工作在 OSI 模型的第三层。

network monitor (NetMon，网络监视器) 与 Windows NT Server 4.0 或 SMS 捆绑的一个网络监视软件，它能完成的工作包括捕获从一个网段或多个网段来的数据，捕获从一个特定节点来的或发往某个特定节点的数据帧。通过发送一定数量和类型的数据而使网络进入一个特定的状态，检测其他正在运行的 NetMon 的副本，产生关于网络行为的数据。

Network News Transfer Protocol (NNTP，网络消息传输协议) 支持新闻组协议、发送新消息和不同新闻服务器之间传输文件的协议。

Network operating system (NOS，网络操作系统) 运行在网络服务器上的软件，能够使服务器管理数据、用户、组、安全性、应用程序和其他网络功能。最流行的网络操作系统(NOS)是微软的 Windows NT 和 Novell 的 NetWare。

network termination 1 (NT1，网络终端) 在 ISDN 网络上应用的一种设备，用来把引入的双绞线和用户的 ISDN 终端设备连接起来。

network termination 2(NT2) 在 PRI 上为操作多条 ISDN 线而设的附加设备，多条 ISDN 线是连接在用户终端和当地电话公司的电话线之间的。

network transport systems (网络传输系统) 用于定义数据打包并在介质上传输的一系列规定。

network virus (网络病毒) 一种利用网络协议、命令、邮件程序来传播的病毒。虽然从理论上讲，所有的病毒都可通过网络传输，但是网络病毒却是专门攻击网络的。

NetXRay Network Associates 公司的网络分析器软件，可以进行数据捕获和分析，发现节点，查找流量趋势、历史并能进行预测。

newsgroups(新闻组) 一种类似于 E-mail 的 Internet 服务。提供了一种发送消息的方法，但又与 E-mail 不同，可以从一个用户同时发送给一组数目可以很大的用户。

NFS(Network File System，网络文件系统) 一个客户机/服务器应用程序，允许用户在远程机上浏览、保存或更新文件，就好像在本地机一样。可以用来安装 Linux。

node(节点) 连在网络中的计算机或其他设备。

noise (噪声) 不规则信号或干扰，源于网络电缆附近的电动机、电力线或雷达。

nslookup(一个 TCP/IP 的应用程序) 允许用户通过指定的 IP 地址来查找相应网络节点的 DNS 名。对确定一个主机是否配置正确或解决 DNS 解析问题非常有用。

NTFS(New Technology File System，新技术文件系统) 微软公司主要为 Windows NT Server 和 Windows NT workstation 开发的文件系统。NTFS 集成了操作文件的可靠性和压缩能力，绝大多数的 Windows NT Server 既支持 FAT 又支持 NTFS。

O

object(对象) NetWare Nds 树上的一个资源。一个对象可以代表一个组、一个用户、一个打印阵列、一个服务器卷、一个用户模板和一个邮箱。它可以包含或不包含其他对象。所有的对象在 NDS 中可以集中管理。

octet 组成 IP 地址的 4 字节之一。

one-way domain trust relationship (单向域委托关系) 一个域允许另一个域的用户访问自己的资源，但是反过来不行。

online backup(在线备份) 在 Internet 上把数据备份到一个中心位置的技术。

online UPS (在线式 UPS) 一种电源，不断地用交流电给电源的电池充电，而电池给网络设备供电。

Open Shortest Path First(OSPF，最近优先协议) 组成 RIP 的一些限制并和 RIP 在网上共享的路由协议。

open source software(开发源码软件) 一个用来描述那些在分发上没有限制，并且公布源代码的软件的词汇。

Open Systems Interconnection(OSI) Model (开放系统互联模型) ISO 组织在 20 世纪 80 年代发展的，用来理解和发展计算机通信的模型。它把网络模型分为 7 层：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

Orange Book(橙皮书) 美国国防部在 1985 年公布的计算机操作系统的规定。

organizational unit 参考 Container Object。

owner(业主) 对工程在预算内按时完成负责的人。

P

Packet Internet Groper(PING，因特网包探测器)　一个 TCP/IP 查错工具，它可以确认 TCP/IP 是否安装，是否绑定到网络接口卡，是否配置正确以及能否与其他计算机通信。使用 ICMP 发送显示请求并得到回答信息，从而判定 IP 地址是否有效。

packet-filtering firewall(包过滤式防火墙)　一个工作于传输层和数据链路层的路由器。它检查每个数据包的头来决定是否是授权的数据包。如果是授权数据包就把它发往目的地址；否则过滤掉。包过滤式防火墙也叫作屏蔽防火墙。

packet switching(包交换)　一种交换方式，数据在传输之前先打包。因为每个包都含有目的地址和校验信息，所以在包交换中，数据包可以通过任何一条路径到达目的地。

parallel backbone(并行主干)　最具健壮性的企业级拓扑结构，从中心路由器到每个网段都有不止一个连接。

parity(奇偶校验)　一种用来验证数据完整性的机制，通过把所存的位计算得到一个奇或偶的值来完成。

parity error checking(奇偶校验检查)　比较从磁盘读来的数据的奇偶性与系统所使用奇偶性的过程。

partial synchronization(部分同步)　一种类型的同步，只将用户账户信息改变了的部分在域控制器之间进行传递。也就是说，主域控制器(PDC)和备份域控制器(BDC)发现了它们数据间的差异并解决的过程，部分同步是自动发生的。

passive hub(被动式集线器)　在网上简单地放大所传输数字信号的集线器。

patch(补丁)　对软件程序一部分的升级，经常是由软件供应商发布的。以便解决软件代码中的问题或增加更多功能。

patch cable(转接电缆)　一段比较短的两头都有转接头的双绞线电缆(一般为 3～50 英尺)，可用于把网络设备连接到数据口。

patch panel(插口面板)　安装在墙上的面板，上面有供数据接收模块的交叉电缆插入的接口。

PC Card　参考 PCMCIA。

PCMCIA　20 世纪 90 年代早期由国际个人电脑存储组织提供，用来连接手持电脑部件的接口。PCMCIA 提供的插槽可以连接 Modem 卡、网络接口卡、外接硬盘或 CD-ROM 卡。

peer to peer communication(点对点通信)　网络计算机使用一根电缆进行通信的简单方法。在点对点通信中，没有一台计算机有比其他计算机更高的权限，所有的计算机都对等地与其他计算机共享文件。

per seat(每客户)　一种 Windows NT Server 的授权模式，允许限定数目的客户端同时访问服务器(数目取决于购买 Windows NT Server 时的授权协议)。授权限制不是对授权客户端的而是限定同时连接的数目。

Peripheral Component Interconnect(PCI，外围器件互联总线)　20 世纪 90 年代提出的 32 位或 64 位总线。新生产的网络接口卡几乎都采用 PCI 总线。它比 ISA、MCA、EISA 都要短，但却有快得多的数据传输能力。

phase(相位)　对波传播的一种度量。可通过在时间上和对其他波进行对比得到。

physical layer(物理层)　OSI 模型的最底层或第一层。物理层包含网络的物理介质，如电缆和接头。

physical memory(物理内存)　安装在计算机主板上为计算机提供专用存储的芯片(与虚拟内存相对应)。

physical topology(物理拓扑)　网络的物理结构。物理拓扑从一个全面的角度描述网络，它不定义设备连接方法或地址。物理拓扑分成 3 个基本拓扑：总线型、星型和环型，这些基本的拓扑可以互相组合形成复杂的拓扑结构。

pilot network(原型网络)　一种代表大型网络的小型网络。它可以用来评价网络改变或增加设备对网络的影响。

pipe(管道)　一种 UNIX 系统工具，它可以使用户连接多个命令从而形成一个新的命令，以实现系统没有的功能。它是 UNIX 系统最强有力的工具之一。

pipe line(管道行)　一系列由管道符连接起来的多个 UNIX 命令。

plain old telephone service(POTS，旧式电话服务)　参考 PSTN。

plenum(通气层)　在楼板和天花板之间的区域。

point of presence(POP，接入点或连接点)　两个电话系统(如长途载波电话与一个本地电话公司，或者本地载波电话与 ISP 设备)相交的地方。

Point-to-Point Protocol(PPP，点对点协议)　一种可以使工作站通过串行接口接到服务器上的通信协议。PPP 支持多个网络层协议，可以使用同步或异步通信，且不需要在客户端工作站上进行很多设置。

Point-To-Point Tunneling Protocol(PPTP，点对点隧道协议)　由微软发展的第二层协议，它使 PPP 可以在 Internet 上以传输标准 IP 包的形式传输任何类型的数据。PPTP 支持加密、验证和由 RAS 提供的局域网访问。使用 PPTP，用户可以拨号到他们的 ISP，然后通过 Internet 来访问他们公司的局域网，而不必拨号访问服务器。

polymorphic virus(变形病毒)　一种类型的病毒。每次传输到一个新系统时它都会改变其特点(如字节安排、大小及内容命令)，使它更难以辨认。

port(端口)　一个主机地址，在这个地址上一个应用程序可以输入数据。

Post Office Protocol(POP，邮局协议)　一个 TCP/IP 的子协议。提供 E-mail 消息的集中存放，类似于在传统邮政系统中的邮局，信件被投递之前都存放在邮局。

predecessors(前趋)　在一个工程中必须在别的任务开始之前完成的任务。

presentation layer(表示层)　OSI 模型的第六层，作用相当于应用程序和网络之间的一个翻译。在这个层上，数据根据所使用网络的类型被表示为网络可以理解的格式。表示层还管理数据的加密和解密，如加密系统密码。

Pretty Good Privacy(PGP，更好地保密隐私)　一个基于密匙的、使用两步验证过程的 E-mail 加密系统。

Primary Rate ISDN(PRI，基本速率 ISDN)　一种使用 23 个数据通道和一个 64kb/s 数据通道的 ISDN，经常被表示为 23B+D。PRI 在个人用户中不如 BRI 用户普遍，它主要用在商业或公司等需要较大带宽的地方。

primary domain controller(PDC，主域控制器)　一台集中管理全域账号和安全信息的计算机。一个域中只能有一个主域控制器(PDC)。

print services(打印服务)　一种允许网上多个用户共享打印机的网络服务。

process management(进程管理)　以一种系统的方法计划、实施和完成任务的步骤。在工程实现过程中可以被管理的进程包括变换、支持、培训、代表和问题解决。

project management(项目管理)　对资源、人员、预算和其他方面进行管理，以便在给定约束的条件

下完成任务的实践行为。

project plan(项目计划)　有关一个项目管理细节的组织方法。有些项目计划是通过软件实现的，如微软的 Microsoft Project。

promiscuous mode (混合模式)　网络接口卡的一种特性。它允许网络接口卡为一个设备驱动程序截获所有在网上传输的帧，而不仅仅是以自己为目标的帧。

promote(提升)　微软的一种术语。指一个域内提升一个服务器权限的过程。例如，如果一个主域控制器(PDC)失败，管理员也可以把一台备份域控制器(BDC)提升为主域控制器(PDC)。

proprietary UNIX(专用 UNIX)　UNIX 的实现方法，其中仅根据从 The Santa Cruz Operation 购买授权副本的情况来决定原码是否可用(成本高达数百万美元)。

protected mode(保护模式)　NetWare 的一种运行形式，它在与操作系统相隔离的内存区域内运行服务。在保护模式下运行服务可以防止有的服务使服务器失败。在保护模式下，服务器及支持的程序不会影响系统进程。

protocol(协议)　网络用来传输数据的规则，协议保证数据完整、顺序、无错地在网络节点之间传输。

proxy server(代理服务器)　一种运行代理协议的网络主机。代理服务器也称网关。

proxy service(代理服务)　一种运行于网络主机的程序。作为网络内部和外部的接口，监视所有进出网络的流量，对外部网络提供一个 IP 地址，而不是把整个局域网的 IP 地址暴露给外部。

PSTN(Public Switched Telephone Network，公用电话交换网)　由一般电话线组成的网络，已经工作了近 100 年，而且现在许多家庭还在使用。

punch-down block(下行块)　一块面板，上有供工作站电缆连接的插头。

PVC(Private Virtual Circuit，个人虚拟电路)　一种与专线相对的点对点的连接，数据可能经过多条不同路径到达目的地。X.25、帧中继和某些类型的 ATM 使用 PVC。

R

radio frequency(RF，射频)　一种依赖于特殊的频率广播的数据传输方式，与电视或电台的工作方法相同。RF 可以使用宽带或窄带技术。

radio frequency interference (RFI，射频干扰)　一种类型的干扰，由马达、电力线、电视、复印机、日光灯或电台和电视台产生。

RAID Level 0 (RAID 0)　RAID 技术的一种，数据以 64KB 大小的块均匀分布在磁盘阵列中。

RAID Level 1 (RAID 1)　RAID 技术的一种，通过使用磁盘镜像来提供数据冗余，当数据写入一个磁盘时自动在另一个磁盘上保留备份。

RAID Level 3(RAID 3)　RAID 技术的一种，使用磁盘条带化，把奇偶校验位写在一个单独的磁盘上。

RAID Level 5(RAID 5)　当今最流行的，提供最好容错性能的数据存储技术。RAID 5 把数据分成小块写在多个磁盘上，同时也把奇偶校验信息写在多个磁盘上。

real-time (实时操作系统)　一种操作系统，它最少包括两种特征：对外界事件的感知能力(如感知温度的变化)和对这些事件在可预测时间内的反应的能力(如在 3ms 内打开热机)。

reassembly (重组)　把分段的数据块重新组织起来的过程。

redundancy (冗余)　使用一个以上的部件存储、处理、传输数据。

Redundant Array of Inexpensive Disks (RAID，廉价磁盘冗余阵列)　一种服务器的冗余技术，使用多个物理磁盘或逻辑磁盘保证数据的完整性和访问效率。有些 RAID 设计能提高存储器容量和系统性能。参考 disk striping(磁盘条带化)和 disk mirroring(磁盘镜像)。

regeneration (再生)　重新传输一个数字信号的过程。再生与放大不同，它只重复信号，噪声并不会积累。

release (释放)　中断一个 DHCP 租用的行为。

remote access (远程访问)　给雇员、通信提供者或远程供应商提供通过远程访问服务器访问一个组织内部的局域网或广域网的能力。

remote access server (远程访问服务器)　用来提供多个用户拨入局域网或广域网的硬件和软件的结合。

remote access service (RAS，远程访问服务)　最简单的拨入服务器之一，这个软件包含在 Windows NT Server 中。注意“RAS”发音为“razz”。

Remote Authentication Dial-In User Service (RADIUS，远程拨入用户验证服务)　为网络访问服务器(可能为 Windows NT 或 Novell 远程访问服务)提供用户身份验证的一台服务器。

remote computer(远程计算机)　通过网络连接工作或控制的计算机。

remote control(远程控制)　一种远程访问的解决方案，远程用户拨入一台直接连接在局域网上的工作站，运行于该工作站和远程用户计算机上的软件允许用户接管该工作站。

remote node(远程节点)　直接拨号到一个局域网的远程访问服务器的一台客户机，LAN 把该节点与其他点同样对待，允许远程用户完成他或她在办公室中同样的工作。

remote user(远程用户)　工作于一台在地理上不同于局域网服务器的计算机上的人。

repeater(中继器)　一种用来重生和放大模拟或数字信号的连接设备。

resolver(解析者)　任何需要在 Internet 上查找信息的主机。

resource record(资源记录)　在一台命名服务器上的 DNS 数据库中存储的元素，包含 TCP/IP 主机名和它们的 IP 地址信息。

restore (恢复)　在文件丢失或被删除后从备份中重新复制的过程。

Reverse Address Resolution Protocol (RARP，逆向地址解析协议)　逆向的 ARP。RARP 允许客户机发送一个包含自己 MAC 地址的广播信息以得到 IP 地址。

ring topology(环型拓扑)　一种网络设计，每个节点与两个最近节点相连，使整个网络组成一个环，数据在环中单向传输，每个工作站接收并应答发送给它的包，然后把包发送给环中的下一个工作站。

ring WAN topology(环型广域网拓扑)　一种广域网拓扑，每个站点与另外两个站点相连，使整个广域网组成一个环型。这种结构与局域网中的环型拓扑类似，不同之处在于广域网拓扑连接的是两个远程站点，而局域网环型拓扑连接的是本地节点。

risers(上行线)　提供楼层之间垂直连接的主干网电缆。

root(root 用户)　一个很高权限的用户 ID，有权建立、删除、改变、移动、读写或执行文件。这个用语可以指 UNIX 网络的管理员。

root server(根服务器)　一台由 InterNIC 维护的域名服务器，决定最高层的域名，如那些以.com、.edu、.net、.us 等为后缀的。InterNIC 在全世界维护 13 台根服务器。

routable(可路由的)　可以在多个网上传输的协议，因为它们携带可被路由器处理的网络层地址信息。

route (路由)　根据地址、应用模型或子网的可用性在网间传输数据。

router(路由器)　一个可以连接多个以不同的传输速率和不同的协议运行的局域网或广域网的多端口设备。另外，路由器可以判定数据传输的最佳路径，也可以完成一些高级管理功能。路由器工作在 OSI 的第三层或更高层，它们是智能的、与协议无关的设备。

routers(路由器组) 连接不同网段，根据数据帧中包含的信息智能地传输数据的设备组。

Routing Information Protocol(RIP，路由信息协议) 最古老的但如今还在广泛使用的路由协议。与其他路由协议相比，RIP 较慢而且安全性较差。

Routing Protocols(路由协议) 路由器之间传输信息的方法。路由协议判定数据在节点之间的最佳路径，它们与可路由协议如 TCP/IP 和 IPX/SPX 不同，尽管它们可能工作在可路由协议上。

routing switch(路由交换机) 第三层或第四层交换机的别称，它可以与路由器或交换机协同工作，因而可以处理从第二层到第四层的数据。

runts 比传输介质规定的最小尺寸还要小的数据包，如任何小于 64B 的以太网数据包都被认为是一个 runt。

S

Samba 一个开放源码软件包，提供完全类似 Windows NT 风格的文件和打印机共享工具。

schema 一个网络逻辑设计的参考，一个在 NDS 树的产生、使用、对象设计、层次规则和策略(如安全水平)等方面具有指导作用的模式。

screening firewall 参见 packet-filtering firewall。

SDH(Synchronous Digital Hierarchy，同步数字树) 国际的 SONET 等价物。

Secure Sockets Layer(SSL，安全套接层) 当 Web 页在 Internet 上传输时对其加密的一种方法。

security audit(安全审查) 对一个组织的安全防范的评价，安全审查应该最少每日(推荐为每刻钟)进行一次。对每个发现的隐患，要衡量其严重性并找出与其相类似的隐患。

security auditing(安全审查) 在网络上衡量现在的安全性，并且当崩溃发生时通知管理员。

segment(网段) 在局域网中与其他局域网部分隔离的一部分，共享一个固定的传输容量。

segmentation(分段) 当能处理较大数据单元的网段发送数据到只能处理较小数据单元的网段时把数据单元的长度变小的过程。

self-healing(自适应) 双环拓扑的一种特征，允许当主环失败时自动在备份环上重传。

Sequence Packet Exchange(SPX，序列包交换) IPX/SPX 协议栈的核心协议。SPX 是属于 OSI 模型中的传输层的协议，与 IPX 协同工作，保证数据完整、顺序无错地传输。

sequencing(序列) 给每一块数据赋予一个序列号，从而可以使接收方的传输层能根据序列号以正确的顺序重组数据。

serial backbone(串行主干网) 最简单的主干网类型，由两个或多个集线器相互之间用一根电缆连接组成。

Serial Line Internet Protocol(SLIP，串行 Internet 协议) 使一个工作站与一台服务器通过一条串行线连接起来的通信协议。SLIP 只支持异步通信和 IP 传输，并且在客户端需要更多的配置。

server(服务器) 在网上管理共享资源的计算机。服务器通常比客户机拥有更强大的处理能力、更多的内存和硬盘空间，它们运行的网络操作系统(NOS)，不但能管理数据，而且能够管理用户、组、安全性和应用程序。

server-based network(基于服务器的网络) 使用特殊的计算机(文件服务器)来为其他的计算机提供数据和通信的网络。

server clustering (服务器集群) 一种容错技术，把多个服务器连接在一起，作为一个单独的服务器。在这种配置中，集群服务器间分配处理任务，对用户而言就像一台服务器。如果一台服务器失败，其余服务器会自动接管它的数据事务和存储任务。

server console (服务器控制台) NetWare 服务器上对网络管理员的主要接口。与 Windows NT 不同，NetWare 服务器的界面不是全图形化的。NetWare 4.x 只提供基于文本的菜单，NetWare 5.0 允许用户既可以通过文本方式也可以通过图形方式来访问命令。

server mirroring (服务器镜像) 一种容错技术。一台服务器把自己的事务和数据完全复制在另一个服务器上，服务器镜像要求在两台服务器之间和两台服务器上运行的软件之间建立连接，以便两台服务器保持同步，如果一台服务器失败，另一台会接续它的工作。

Service Access Point(SAP，服务访问点) 以太网的一种特征，用来标识一个使用 LLC 协议的节点或内部进程。每个源节点和目的节点之间的进程需要一个唯一的 SAP。

Service Advertising Protocol(SAP，服务器广告协议) IPX/SPX 协议的一个核心协议，工作在 OSI 模型的应用层、表示层、会话层和传输层，并且直接运行于 IPX 之上。NetWare 服务器和路由器通过 SAP 来向全网通告自己的服务。

service pack (服务补丁) Windows NT 的重要补丁。

services (服务) 网络提供的特征。

session (会话) 在两部分之间交换数据的连接。经常用于描述终端和主干之间的连接。

session layer (会话层) OSI 模型的第五层。会话层在网络上的两个节点之间建立并保持通信，可以被认为是网上的“交通警察”。

sheath (绝缘层) 电缆的外层或包裹的绝缘皮。

shell (外壳) 命令执行器的别名。

shielded twisted-pair (STP，屏蔽双绞线) 一种类型的电缆，由一对相互扭绞的线组成，线的外面包了一层金属屏蔽层，屏蔽的作用像天线一样把噪声转化为电流(假设电缆正确地接地)，这个电流产生一个与双绞线内电流大小相等、方向相反的电流。在屏蔽网上的噪声镜像双绞线的噪声，并相互抵消。

signal bounce (信号反射) 在一个总线网上，信号在两个端之间无休止传播的现象。在每端使用 50Ω 的电阻能够阻止信号反射。

signal level (信号电平) 一个 T 载波的 ANSI 标准，规定物理层电信号的特征。DSO 等价于一个数据或语音通道，其他信号电平是 DSO 的整数倍。

signature scanning(特征扫描) 通过比较文件内容和已知病毒特征(病毒的特征代码)来决定该文件是否有病毒。

simple installation(简单安装) 一个 NetWare 的安装选项，其中最常用的安装内容被选中，而且耗时比自选安装要少。

Simple Mail Transfer Protocol (SMTP，简单邮件传输协议) TCP/IP 的子协议，负责在 E-mail 服务器之间传输信息。

Simple Network Management Protocol (SNMP，简单网络管理协议) 用来管理 TCP/IP 网络设备的通信协议。

single domain model (单域模型) 最简单的 Windows NT 域模型，由一个服务、一个组织的所有用户和资源的域构成。

single-mode fiber (单模光纤) 一种类型的光纤，使用单一频率的光纤从一端到另一端传输数据。数据在单模光纤中比在多模光纤中传输更快、更远，但单模光纤相当贵。

single point of failure (单独失败点) 在网络上的一个地方，如果一个错误在此发生，数据传输将中断且不能自动恢复。

sneakernet(人工传递网络)　没有网络时数据交换的唯一方法，要求把数据复制到一张软盘，把软盘带到另一台计算机，然后把软盘的数据备份到此计算机。

sniffer (网络探测器)　一台装有特殊网络接口卡和网络分析软件的手提电脑。与装有网络监视工具的手提电脑不同，它一般不能用于其他的目的。因为它并不依赖于像 Windows 之类的网络操作系统(NOS)。

social engineering (保安员)　管理与网络安全环境和系统访问有关的问题。

socket (套接)　赋予在一台主机上运行的进程一个逻辑地址，它组成一个在主机和客户机之间的虚拟连接。

soft skills(软技能)　像客户关系、领导才能和独立性之类难以测量，但又很重要的技能。

software distribution (软件分发)　把一个数据文件或程序自动从服务器传到客户机的过程。

SONET (Synchronous Optical Network，同步光纤网)　一种广域网技术，使用与 T 载波相同的时分复用方法，提供从 64kb/s～2.4Gb/s 的数据传输。SONET 是在北美、欧洲、亚洲之间进行广域网连接时的最佳选择。因为它可以直接连接不同的标准、不同的国家。

Source Route Bridging (源路由桥)　在大部分令牌环网络中使用的桥接方法。

spike　在衡量网络性能时的一个单个的跳变。

sponsors (赞助商)　一个负责诸如支持工程、提高预算、同意工程延期、与提供商谈判等的人。

spread spectrum (扩频)　一种类型的射频传输，使用低电平的、扩展在多个频率的信号。扩频比一般的窄带传输安全性高。

stackable hub (堆叠式集线器)　一种类型的集线器，设计用来与其他的集线器相互连接而组成一个逻辑上更大的集线器。

stakeholder　任何被一个工程所影响的人，无论是有益还是有害，可以是工程的参与者、用户、管理者或设备提供商。

standalone computer(独立的计算机)　一台只使用自己本地磁盘上的程序或数据而不连接到网络上的计算机。

standalone hub(独立的集线器)　一种设计只用来为一组计算机服务而与网络的其余部分相隔离的集线器，这种集线器可以通过同轴电缆、光纤或双绞线与其他集线器相连，一般不用于树型或链式网络。

standards (标准)　包含技术定义和其他精确标准，用来指导或保证物质、产品、过程和服务能达到设计目标的文档。

standby UPS (后备式 UPS)　通过在电源掉电时立即切换到用电池供电，从而为设备提供持续的电源的 UPS。当电源恢复时，旁路式 UPS 又切换回用交流电源供电。

star topology (星型拓扑)　一种类型的物理拓扑，每个网络中的节点都连接到一个中心设备(如集线器)。在星型拓扑中，每个单独的电缆都只连接两个节点，所以一个电缆的问题只会影响两个节点。节点把数据发送到中心集线器，然后由中心集线器把数据发送到网络的其他地方。

star WAN topology (星型广域网拓扑)　与局域网中的星型网络拓扑非常相似的一种广域网技术，一个单独的站点作为中心连接着多个站点。

star-wired bus topology (星型总线拓扑)　一种混合的拓扑结构，工作站以星型方式连接到集线器上，集线器之间以总线形式相连。

star-wired ring topology (星型—环状拓扑)　一种类型的混合拓扑，使用星型的物理设计，使用令牌环

作为数据传输方法。

static IP address (静态 IP 地址) 手动指定给一个设备的 IP 地址。

stealth virus (隐藏型病毒) 一种类型的病毒，它把自己隐藏起来以避免检查。一般来说，隐藏型病毒把自己隐藏在合法程序中或用自己的带破坏性的代码取代合法程序的一段代码。

store and forward mode (存储发送模式) 一种交换方法，交换机把整个数据帧读入内存并检验它的正确性然后发送。这种模式比随时发送模式花费更多的时间，但传输数据更准确。

structured cabling(结构化布线) TIA/EIA 508 定义的、标准的、企业级的、多厂商环境的布线方法，是商业大楼的布线标准(Commercial Building Wiring Standard)。结构化布线是建立在以高速骨干网为基础的结构化设计基础上的。

subnet mask(子网掩码) 一种特殊的 32 位二进制数，与 IP 地址相结合可以通知网络的其余部分该设备属于哪一个子网。

subnets(子网) 在 Internet 上，单独的网络之间是通过路由器相互连接的。

subnetting(划分子网) 把一个网络划分为多个更小的网络的过程。

subprotocols (子协议) 属于一个协议栈并与其他协议协同工作的小的协议。

supported services list (支持服务列表) 列出在一个组织内所支持的所有服务或软件包的文档(一般为在线的)，在名字后加上第一个“-”和第二个“-”可以支持对这些服务或软件包的访问。

surge (浪涌) 由于远距离的闪电或电路问题引起的电压突然升高。

SVC(Switched Virtual Circuit，虚拟交换电路) 一种逻辑的点对点连接，依靠交换机来判定最佳路径。ATM 使用 SVC。

switch(交换机) 管理网络交换的硬件设备，用于把网络隔成多个小段，每个小段支持自己内部的相互传输而与其他的小段隔离。

switched Ethernet(交换式以太网) 一种新的以太网模式，因为通过交换指定了多个逻辑上相互隔离的网段，多个节点可以同时发送或接收数据，从而利用了更大的带宽。

switching (交换) 网络逻辑拓扑的一个元件，用于管理数据包如何过滤和发送。

symmetric multiprocessing(对称多处理器) 实现多线程的一种方法，它通过把所有的操作平均分配给两个或多个处理器来完成。Windows NT Server 支持这种方式。

symmetrical (对称的) 传输技术的一种特征，为数据上传和下载提供同样的容量，适合那些既要上传又要下载的用户。

symmetrical DSL(对称 DSL) DSL 技术的一种，为在用户和服务提供者之间的上传和下载提供同样的容量。

synchronization(同步) 主域控制器(PDC)和备份域控制器(BDC)之间为了保持两者所维护的用户账号信息相同而采取的同步措施。

synchronous(同步模式) 一种传输方法，数据在发送者和接收者之间传输时必须有时钟同步。

T

T-carriers(T 载波技术) 描述任何类型的符合 T1s 标准的专用线路的名词，包括 T1s、T1cs、T2s、T3s、T4s。

T1 T 载波技术的一种，提供 1.544Mb/s 带宽和 24 个通道，可以传输话音、数据、视频或音频信号。T1 可以使用屏蔽的或非屏蔽的双绞线、同轴电缆、光纤或微波信道，商业公司一般用 T1 与它们的 ISP 相连。电话公司一般使用最少一条 T1 与它们的中央办公室相连。

T3　T 载波技术的一种，可以传输 672 个通道的话音、数据、视频或音频，最大有 44.736Mb/s(为了讨论方便一般认为是 45Mb/s)的容量。T3s 要求光纤或微波信道。

TCP segment (TCP 段)　TCP/IP 数据包中包含 TCP 数据的部分，由 IP 层封装。

TCP/IP core protocols (TCP/IP 核心协议)　TCP/IP 的子协议。

Telnet　一个终端仿真协议，用来使用 TCP/IP 登录远程主机。Telnet 在 TCP/IP 协议栈的应用层。

terminal (终端)　一台几乎不具有自己的处理能力或存储能力的设备，需要靠一台主机来提供应用程序和数据处理服务。

Terminal Access Controller Access Control System (TACACS，终端访问控制器访问控制系统)　为远程访问服务器提供的一个集中的身份验证系统，与 RADIUS 相似。

terminal adapter (TA，终端适配器)　用来把数字信号转换成模拟信号的设备。一般在 ISDN 或其他模拟设备中使用。终端适配器有时候被错误地称为 ISDN 调制解调器。

terminal equipment (TE，终端设备)　用来把计算机连接到 ISDN 线上的设备。终端设备可以包括独立的设备或插卡(与以太网和令牌环网中使用的网络接口卡相似)或 ISDN 的路由器。

terminator (终端器)　在总线的末端的一个电阻，当信号到达传输目的后用来吸收信号能量。

thicknet (粗缆)　一种类型的同轴电缆，也叫作粗以太网，是一根较硬的电缆，大概 1cm 粗。粗缆是以太网最早使用的电缆类型，因为它们经常包裹着一层黄色的绝缘层，所以也称为黄以太网。IEEE 把粗缆定义为 10Base-5 以太网，10 代表 10Mb/s 的带宽，Base 代表基带传输，5 代表无中继的最大网段长度为 500m。

Thinnet (细缆)　一种类型的同轴电缆，也称为细以太网。20 世纪 80 年代是局域网中最流行的传输介质，与粗缆相同，细缆现在也很少使用。IEEE 定义细缆为 10Base-2 以太网，10 代表数据传输的速率为 10Mb/s，Base 代表基带传输，2 代表细缆的无中继最大网段长度大约为 200m(185m)。

throughput (吞吐量)　介质在给定时间内能传输的数据的数量，通常以兆/秒为单位，或写作 Mb/s。每个传输介质的物理特性决定它的可能的传输容量。

tiered WAN topology (堆叠式广域网拓扑)　一种广域网拓扑结构，站点连接成星型或环型，网与网之间在不同层次上连接组织成多个层。

time division multiplexing (TDM，时分多路复用)　一种类型的多路复用技术，把信道按时间分割成多个通道，给每个数据流赋予不同的通道，在发送端的设备(多路器)组织数据流，在接收端的设备过滤数据还原为原来的形式。

time-sharing system (时间共享系统)　一种计算机系统，用户必须直接连接以共享资源。

token (令牌)　一种特殊格式的帧，一个节点用来通知网上其他的节点自己具有发送数据的权限。

token passing (令牌传递)　一种类型的数据传输，一个 3 字节的数据包(叫作一个令牌)，在网上循环传递。

Token Ring (令牌环)　20 世纪 80 年代由 IBM 发展起来的网络技术。它依赖于节点之间的直接连接形成环型拓扑，使用令牌来决定哪一个节点可以传输数据。

Top-Level Domain(TLD，顶层域)　最高层的用来区分域名的分类，如.org、.com、.net 等。一个顶层域也叫作域后缀。

topology (拓扑)　一个计算机网络的物理设计。

traceroute (或 tracert)　一个 TCP/IP 的网络查错工具。使用 ICMP 跟踪从一个节点到另一个节点的网络路径，判定两个节点之间的断点，对于判定路由器和子网之间的连接问题非常有用。

traffic (网络流量) 在任何给定时间发生在一台网络中的计算机上的数据传输和处理行为。

traffic monitoring (流量检测) 判断在一个网络或网段上有多少处理过程发生，并在网络过载时通知管理员。

Translational Bridging (翻译桥) 连接令牌环网和以太网的一种桥接方法。

transmission media (传输介质) 数据传输和接收所使用的物质。传输介质可以是物理的，如线和电缆；也可以是无形的(无线)，如射频波。

Transparent Bridging (透明网桥) 在大多数以太网上使用的桥接方法。

Transport Control Protocol (TCP，传输控制协议) TCP/IP 协议栈中的核心协议之一，属于传输层，用来提供数据的可靠传输服务。

Transport layer (传输层) OSI 模型的第四层。传输层负责数据可靠无错地从 A 点传输到 B 点(两点可以在同一个网段，也可以不在同一个网段)。

Trojan horse (特洛伊木马) 一个把自己伪装成有用程序的对系统有害的程序。

trust relationship (信任关系) 使一个域中的用户可以访问其他域中的资源的一种设置。一个唯一的安全标识标志每一个域，而且每个域都有自己的安全数据库来跟踪文件和资源的权限。

tunneling (隧道) 把一个协议封装使其看起来像另一个协议的过程。

twist ratio (绞扭率) 在双绞线上每米或每英尺相互绞扭的次数。

Twisted-Pair (TP，双绞线对) 一种类似于电话线的电缆，由带有彩色绝缘皮的铜线对组成，每个铜线有 0.4～0.8mm 粗，相互绞扭，封装在塑料中。

twisted-pair cable(双绞线电缆) 最便宜的局域网电缆，由 4 对相互绞扭的带绝缘皮的线组成。两个相互绞扭的线组成一个线对，一个用于传输信号；另一个接地，用来吸收干扰。

two-way domain trust relationship (双向域委托关系) 两个域允许相互访问资源的设置。双向域委托关系在广域网中使用很普遍，两个或多个站点管理它们自己的域，但需要共享信息。

typeful (带类型标识的缩写方法) 一种表示对象的缩写方法，其中包括组织和组织单位标识(分别为 O 和 OU)。例如，在 Inv.Ops.Corp.Sukin 中，OU = Inv，O=Ops，OU=Corp，O = Sukin。

typeless (不带类型标识的缩写方法) 一种表示对象的缩写方法，其中组织和组织单位被省略，如 Inv.Ops.Corp.Sukin。

U

Uniform Resource Locator (URL，统一资源定位符) 一种标准的用来标识每个 Web 页面的方法。标识服务、主机名和 HTML 页或脚本名。

Uninterruptible Power Supply(UPS，不间断电源) 一种电池操作的电源，直接连接在一个或多个设备和交流电源上。它可以防止非预见性的电源问题对设备造成的损害。

Unqualified Host Name (非确认主机名) 一个 TCP/IP 主机名，不带有它的前缀和后缀。

unshielded twisted-pair (UTP，非屏蔽双绞线) 一种由一个或多个相互绞扭的线对封装在塑料中组成的电缆。像它的名字提到的，UTP 不包含屏蔽层，所以 UTP 比 STP 便宜，但抗干扰性也相对较差。

upgrade (升级) 对一个软件程序现有代码的一个大的改动，由软件提供商免费或付费提供，可以和原来的代码兼容或不兼容。

upstream (上传) 用来描述数据从用户传到本地 POP 局的名词。在非对称通信中，上传使用的容量比下载小得多；在对称通信中，两者是相同的。

User Datagram Protocol (UDP，用户数据报协议)　TCP/IP 协议栈的一个核心协议，属于在 Internet 层和应用层之间的传输层。UDP 是一个面向无连接的传输服务。

user (用户)　一个使用计算机的人。

V

vault　一个大的磁带存储库。

Virtual Local Area Network(VLAN，虚拟局域网)　一种交换机可以使用它来把许多端口逻辑地划分为一个广播域的方法。一个 VLAN 可以由服务器、工作站、打印机、路由器或其他可以连接到交换机的设备构成。

virtual memory (虚拟内存)　从硬盘上划分出一块用作内存(与物理内存相对)。

Virtual Private Network (VPN，虚拟专用网)　一个逻辑组成的广域网，使用现有的公用传输系统，VPN 可以用软件或软件与硬件的结合来实现。这种类型的网络允许一个组织在 Internet 上实现自己的广域网，或(通过租用专用线路)只为自己的办公室服务，并能保证数据安全地与公共网隔离。

virus (病毒)　一种程序，能复制自己感染计算机，通过网络或软盘传播。病毒可以破坏文件或系统，或者只是简单地通过在显示屏上闪烁消息、图片或使键盘发出响声来干扰用户。

virus hoax (病毒欺骗)　通过一个奇怪的或错误的警告消息，病毒可以对用户的工作站进行严重的破坏。

Voice over IP(VoIP)(通过 IP 网络来传输话音)　参见 Internet Telephony。

Volt-amp (VA)(伏特安培)　电力的一种测量单位。一个伏特安培是由一条电力线上的电压和电流产生的。

W

WAN link (广域网连接)　在广域网中用来把一个站点与其他站点连接起来的线。

WAN topology (广域网拓扑)　一个广域网的物理设计。

Wide Area Network (WAN，广域网)　连接一个地理范围内的计算机的网络，可以是一个组织内的，也可以不是。

Windows Internet Naming Service (WINS，Windows 机器在 Internet 上的命名解析服务)　解析机器的 NetBIOS 名为它的 IP 地址的服务。WINS 在 NetBIOS 的系统中普遍使用，所以通常在安装 Windows 操作系统的系统中见到 WINS。

wireless (无线)　通过红外线或射频传输信号的网络。

wizard (向导)　一个简单的图形化的程序，用来帮助用户完成复杂的任务，如在服务器上配置一个网络接口卡。

workstation (工作站)　一台运行桌面操作系统并连接到网络上的计算机。

World Wide Web (WWW 或 Web，万维网)　Internet 上的服务器组，通过特殊的协议或格式共享资源，交换数据。

worm(蠕虫)　一个在网络上传输的程序，虽然它本身并不会像病毒那样改变其他程序，但它可能携带病毒。

X

X.25　一个模拟包交换的广域网技术，适合远距离传输数据，ITU 在 20 世纪 70 年代中期对其进行了标准化。X.25 可以支持 56kb/s 带宽，它最早被用来在主机和远程终端之间通信。

xDSL　用来指所有的 DSL 的变体的名词。

Z

zone(区)　由一个 DNS 服务器管理的一组计算机。

以数字开头的词语

1 GB Ethernet(兆位以太网)　一种新的高速以太网，由 IEEE 802.3 工作组规定。

1000Mb/s　虽然可以在小段的 UTP(非屏蔽双绞线)上运行，但通常在光纤介质上运行。

10Base-2　一种以太网，根据 IEEE 802.3 标准，使用铜缆作为介质，为总线拓扑。

10Base-2　也叫细网或细以太网，它的名字来源于它以 10Mb/s 的速度传输数据(所以叫“10Base”)和它的网段最大长度为 185m，大约 200m(所以叫“2”)。

10Base-5　最初的以太网标准，它使用总线拓扑和粗同轴电缆，也叫粗网或粗以太网。它的名字来源于它以 10Mb/s 的速度传输数据(所以叫“10Base”)和它的网段最大长度为 500m(所以叫“5”)。

10Base-T　一种以太网类型，它使用双绞线、星型-总线拓扑或树型拓扑。以 10Mb/s 传输数据(所以叫“10Base”)同时需要使用双绞线(Twisted-pair)作为介质(所以后缀为.T)。

100Base-T　IEEE 802.3u 定义的一种新的以太网标准，它使以太网在不做大的投资和结构改变的情况下能把局域网的传输速度提高到 100Mb/s。100Base-T 在星型—总线拓扑或树型拓扑中使用基带传输，像 10Base-T 一样，“T”代表使用双绞线。

100BaseTX　100Base-T 技术的一种。它通过以 10 倍的速度传送信号并且减少数字脉冲间隔和工作站用于 CSMA/CD 的等待和侦听时间来达到 100Mb/s 的传输速度，它要求五类 UTP(非屏蔽双绞线)。

100BaseVG　一种可以 100Mb/s 的速率传输数据的网络模型。与以太网不同，100Base-VG 使用一种有优先级的介质访问方法而不是 CSMA/CD；与 100Base-TX 相同，100Base-VG 使用全部 4 对双绞线，它名字中的 VG 来源于它可以传输语音(“Voice Grade”)。

802.3　关于以太网设备和数据操作的 IEEE 标准。

802.5　关于令牌环的联网设备及数据操作的 IEEE 标准。

14.2　专业英语试题分析

14.2.1　考点辅导

2013 年以来的试题中第 71～75 题一般是完形填空的形式，主要考查应试者结合计算机专业技术知识对全文综合理解的程度和串联上下文的能力、应试者语法知识和对句法结构的辨识能力、应试者的词汇量和词汇运用能力。

具体而言，完形填空主要考查应试者对语篇中句法、词语和短语的把握能力，具有较强的测试性。每一个空处都要通过上下文进行综合考虑，仅仅依靠一个单句往往无法确定正确选项。

语篇的内容往往是对网络技术中协议、通信过程、设备、最新技术等相关知识的描述，需要应试者对这些内容有一定的了解。

1. 完形填空中的句法

计算机英语的完形填空，句法强调时态、语态、倒装、复合，同时要求主语、谓语和宾语结构在数、格等方面的一致性。此外，连接手段包括关系代词、关系副词、连接词等，

要求与整个语篇的行文相一致，起到或承接，或转折，或加强的作用，有着非常突出的个性特征。

时态在描述某项事务的发展历史时，一般采用过去时态；对目前尚使用中的技术，采取完成时态或现在时；对未来技术的展望，大都采用将来时。句中几个受同一时间状态限制的动词时态在表达形式上要保持一致。这里包括并列的谓语动词以及主句和从句中谓语动词在表达形式上的一致。

计算机英语的语篇在描述技术类知识时，语态一般力求客观，采用描述性和被动语态较多。这里要注意只有及物动词及相当于及物动词的词组才有被动语态的表达形式。在并列结构中，同样的语义往往需要同样的语态表达形式。

2. 完形填空中的短语和固定用法

英语中有相当数量的动词短语、介词短语和固定搭配，其来源广泛，搭配方式丰富多变。因此需要应试者从动词入手，熟悉固定搭配，尤其是动词短语；从介词入手，了解介词本身的意义，进而了解同一个介词与不同动词、名词搭配产生的不同或相关的意义；理解固定搭配的外延，增强对语义提示的审查力。

3. 完形填空的答题要领

完形填空的答题要领如下。

(1) 通过首句或出现的核心词汇来推断全文的信息。

短文的首句往往是主题句，或出现了核心词汇，能为理解文章的大意和主要内容提供必要线索。一般首句还提供背景资料，因此要特别注意首句，抓住整个段落的纲要。

(2) 把握文章发展的基本线索。

文章总是按照一定思路发展起来的，而不同的逻辑关系主要依靠使用逻辑连接词来表达。文章如果没有出现内在的逻辑关系，就会出现语义不清、逻辑混乱。所以通过表示逻辑关系的词汇把握文章发展的基本线索是至关重要的。

(3) 借助语法知识和专业背景知识确定正确的词汇选项。

计算机专业英语词汇的考查在试题中占一定比例，词汇选项的设计和文章难度的制定与语法都息息相关。应试者务必借助语法知识和专业背景知识来确定正确的词汇选项。同时注意填入的词汇和文中句子的结构要求相一致。

4. 完形填空的答题步骤

完形填空的答题步骤如下。

(1) 通读全文。

由于完形填空是在考查全面理解内容的基础上运用语言的能力，试题篇幅又较短，所以完全有时间利用通读对全文内容有一个基本的了解。应试者要快速阅读段落，把握基本观点，通读时以浏览为主，可以忽略细节。

(2) 复读答题。

在通读的基础上，应试者最好能立即复读，并结合选项，从语法结构、语义、词义、固定搭配等方面结合专业知识来考虑选项。选定之后，还需要回读。在整个答题过程中，切记全文的整体意义，保持思路的连贯性，从而做出正确选择。

(3) 重读检查。

在确定所有选项以后，一定要重读全文，检查并核实每个选项在整篇文章中没有造成语义、结构、逻辑等方面的差错，确保短文是一个内容连贯、层次清晰、中心思想突出的整体。

14.2.2 典型例题分析

例 14-1 Routing in circuit-switching networks has traditionally involved a static routing strategy with the use of __(71)__ paths to respond to increased load. Modern routing strategies provide more adaptive and flexible approaches. The routing function of a packet-switching network attempts to find the least-cost route through the network , with cost based on the number of __(72)__ expected delay , or other metrics in virtually all packet-switching networks, some sort of adaptive routing technique is used. Adaptive routing algorithms typically rely on the __(73)__ information about traffic conditions among nodes . In most cases, adaptive strategies depend on status information that is __(74)__ at one place but used at another. There is a tradeoff here tween the quality of the information and the amount of __(75)__. The exchanged information itself a load on the constituent networks , causing a performance degradation. (2017 年下半年真题 71～75)

(71) A. only　　B. single　　C. alternate　　D. series

(72) A. hops　　B. sites　　C. members　　D. points

(73) A. exchange　　B. transportation　　C. reception　　D . transmissio

(74) A. rejected　　B. collected　　C. discarded　　D. transmitted

(75) A. packets　　B. information　　C. data　　D. overhead

译文：电路交换网络中的路由传统上涉及静态路由策略，使用单一路径来响应增加的负载。现代路由策略提供了更灵活的方法。分组交换网络的路由功能试图通过网络发现成本最低的路由，其成本基于跳数，预期的延迟或其他度量。在几乎所有的分组交换网络中，使用某种自适应路由技术。自适应路由算法通常依赖于有关节点之间流量情况的信息。在大多数情况下，适应策略依赖于在一个地方收集但在另一个地方使用的状态信息。在信息质量和数据包数量之间有一个折中。交换信息本身就是网络上的负载，会导致性能下降。

答案：(71) B　(72) A　(73) A　(74) B　(75) A

例 14-2 If two communicating entities are indifferent hosts connected by a network, there is a risk that PDUs will not arrive in the order in which they were sent, because they may traverse __(71)__ paths through the network.If each PDUs is given a unique number, and numbers are assigned __(72)__ , then it is a logically simple task for the receiving entity to reorder __(73)__ PDUs on the basis of sequence number. A problem with this schemeis that, with a __(74)__ sequence number field, sequence number will repeat. Evidently, the maximum sequence number must be __(75)__ than the maximum number of PDUs that could be outstanding at anytime. (2017 年上半年真题 71～75)

(71) A. same　　B. different　　C. single　　D. unique

(72) A. randomly　　B. equally　　C. uniformly　　D. sequentially

(73) A. received　　B. sent　　C. transmitting　　D. forwarding

(74) A. various　B. diverse　C. finite　D. infinite

(75) A. smaller　B. greater　C. less　D. more

译文：如果两个通信实体是通过网络连接的无关主机，则存在这样的风险，即 PDU 不会按照它们发送的顺序到达，因为它们可能通过网络穿过不同的路径。如果给每个 PDU 赋予唯一的号码，数字被顺序地分配，那么接收实体根据序号对接收到的 PDU 进行重新排序是一个逻辑上简单的任务。该方案的问题在于，在有限的序列号字段中，序列号将重复。显然， 最大序列号必须大于 PDU 的最大数量才能在任何时候都展示出卓越。

答案：(71) B　(72) D　(73) A　(74) C　(75) B

例 14-3　All three types of cryptography schemes have unique function mapping to specific applications. For example, the symmetric key __(71)__ approach is typically used for the encryption of data providing __(72)__, whereas asymmetric key cryptography is mainly used in key __(73)__ and nonrepudiation , thereby providing confidentiality and authentication. The hash __(74)__ (noncryptic), on the other hand, does not provide confidentiality but provides message integrity, and cryptographic hash algorithms provide message __(75)__ and identity of peers during transport over insecure channels. (2016 年下半年真题 71～75)

(71) A. cryptography　B. decode　C. privacy　D. security

(72) A. conduction　B. confidencc　C. confidentiality　D. connection

(73) A. authenticaton　B. structure　C. encryption　D. exchange

(74) A. algorithm　B. secure　C. structure　D. encryption

(75) A. confidentiality　B. integrity　C. service　D. robustness

译文：所有 3 种类型的密码方案都具有映射到特定应用的独特功能。例如，对称密钥加密方法通常用于保障加密数据的保密性，而非对称密钥加密主要用于密钥加密和不可否认性，从而提供机密性和身份认证。另外，散列算法(非加密)不提供机密性，但提供了消息完整性，而带密钥的哈希算法保障数据的完整性并且能够为点对点信息通过不安全信道传递时提供身份验证。

答案：(71) A　(72) C　(73) C　(74) A　(75) A

例 14-4　Without proper safeguards, every part of a network is vulnerable to a security breach or unauthorized activity from __(71)__, competitors, or even employees. Many of the organizations that manage their own __(72)__ network security and use the Internet for more than just sending/receiving E-mails experience a network __(73)__ —and more than half of these companies do not even know they were attacked. Smaller __(74)__ are often complacent, having gained a false sense of security. They usually react to the last virus or the most recent defacing of their website. But they are trapped in a situation where they do not have the necessary time and __(75)__ to spend on security. (2016 年上半年真题 71～75)

(71) A. intruders　B. terminals　C. hosts　D. users

(72) A. exterior　B. internal　C. centre　D. middle

(73) A. attack　B. collapse　C. breakdown　D. virus

(74) A. users　B. campuses　C. companies　D. networks

(75) A. safeguards　B. businesses　C. experiences　D. resources

译文：如果没有适当的保护措施，网络的每个部分都容易受到来自入侵者、竞争对手，甚至是员工的安全漏洞或未经授权的攻击。很多组织管理自己内部网络的安全，但在使用 Internet 时不仅仅是发送/接收电子邮件会遭遇网络攻击，其中一半以上的公司甚至不知道遭到了攻击。小公司常常自满，已经获得了虚假的安全感。他们通常会对最后一个病毒或最近的恶意网站做出反应，但他们被困在一个情况下，即他们没有必要的时间和资源专注于安全防护。

答案：(71) A　(72) B　(73) A　(74) C　(75) D

例 14-5 The Dynamic Host Configuration Protocol provides configuration parameters to Internet __71__ . DHCP consists of two components: a __72__ for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver __73__ parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation. In “automatic allocation”, DHCP assigns a __74__ IP address to a client. In “dynamic allocation”, DHCP assigns an IP address to a client for a limited period of time. In “manual allocation”, a client’s IP address is assigned by the network __75__, and DHCP is used simply to convey the assigned address to the client.(2015 年下半年真题 71～75)

(71) A. switch	B. terminal	C. hosts	D. users
(72) A. router	B. protocol	C. host	D. mechanism
(73) A. control	B. broadcast	C. configuration	D. transmission
(74) A. permanent	B. dynamic	C. connection	D. session
(75) A. controller	B. user	C. host	D. administrator

译文：动态主机配置协议为互联网上的主机提供配置参数。DHCP 由两部分组成：传递从 DHCP 服务器至主机的具体配置参数的协议以及主机网络地址分配机制。DHCP 是建立在客户机-服务器模型之上的，由指定的 DHCP 服务器向动态配置的主机分配网络地址和传递配置参数。DHCP 支持 3 种 IP 地址分配机制。在“自动分配”机制中，DHCP 分配给客户端一个永久地址。在“动态分配”机制中，DHCP 分配给客户端一个临时性的 IP 地址。在“手动配置”机制中，客户端的 IP 地址是由网络管理员分配，DHCP 仅仅起到配送这个指定的地址给客户端的作用。

答案：(71) C　(72) B　(73) C　(74) A　(75) D

例 14-6 Traditional network layer packet forwarding relies on the information provided by network layer __(71)__ protocols, or static routing, to make an independent forwarding decision at each __(72)__ within the network. The forwarding decision is based solely on the destination __(73)__ IP address. All packets for the same destination follow the same path across the network, if no other equal-cost __(74)__ exist. Whenever a router has two equal-cost paths toward a destination, the packets toward the destination might take one or both of them, resulting in some degree of load sharing. Enhanced Interior Gateway Routing Protocol (EIGRP) also supports non-equal-cost __(75)__ sharing although the default behavior of this protocol is equal-cost. You must configure EIGRP variance for non-equal-cost load balancing.(2015 年上半年真题 71～75)

(71) A. switching B. signaling C. routing D. session
(72) A. switch B. hop C. host D. customer
(73) A. connection B. transmission C. broadcast D. customer
(74) A. paths B. distance C. broadcast D. session
(75) A. loan B. load C. content D. constant

译文：传统的网络层数据包的转发依赖于网络层路由协议提供的信息，或者静态路由，独立决定网络内每一跳的转发决策。转发决策仅仅基于目的客户机的 IP 地址。如果不存在等价的路径，则相同目的地的数据包将沿相同的路径在网络中转发。每当路由器有两条等价的路径通往目的地，数据包可能会选择其中的一条或者两条到达目的地，在一定程度上均衡了负载。增强内部网关路由协议(EIGRP)也支持非等价的负载分担，尽管这个协议默认是等价的。你必须配置 EIGRP 非等价负载均衡的方差。

答案：(71) C (72) B (73) D (74) A (75) B

14.2.3 同步练习

1. CDMA for cellular systems can be described as follows. As with FDMA, each cell is allocated a frequency __(1)__, which is split into two parts: half for reverse (mobile unit to base station) and half for __(2)__ (base station to mobile unit). For full-duplex __(3)__, a mobile unit uses both reverse and forward channels. Transmission is in the form of direct-sequence spread __(4)__ which uses a chipping code to increase the data rate of the transmission, resulting in an increased signal bandwidth. Multiple access is provided by assigning __(5)__ chipping codes to multiple users, so that the receiver can recover the transmission of an individual unit from multiple transmissions.

(1) A. wave B. signal C. bandwidth D. domain
(2) A. forward B. reverse C. backward D. ahead
(3) A. connection B. transmission C. compromise D. communication
(4) A. structure B. spectrum C. stream D. strategy
(5) A. concurrent B. orthogonal C. higher D. lower

2. The traditional way of allocating a single channel, such as a telephone trunk, among multiple competing users is to chop up its __(1)__ by using one of the multiplexing schems, such as FDM. If there are N users, the bandwidth is divided into N equal-sized portions, with each user being assigned one portion. Since each user has private frequency __(2)__ , there is now no interference among users. When there is only a small and constant number of users, each of which has a steady stream or heavy load of __(3)__ this division is a simple and efficient allocation mechanism. A wireless example is FM radio stations. Each station gets a portion of the FM band and uses it most of the time to broadcast its signal. However when the number of senders is large and varying or the traffic is __(4)__, FDM presents some problems. If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. And if more than N users want to communicate, some of them will be denied __(5)__ for lack of bandwidth, even if some of the users who have been assigned a

frequency band ever transmit or receive anything.

(1)	A. capability	B.capacity	C. ability	D. power
(2)	A. band	B. range	C. domain	D. assignment
(3)	A. traffic	B. data	C. information	D. communications
(4)	A. continuous	B. steady	C. busy	D. flow
(5)	A. allowance	B. connection	C. percussion	D. permission

14.2.4　同步练习参考答案

1. **参考译文：**蜂窝系统中的 CDMA 可以如下描述：采用 FDMA，每个蜂窝分配有一个频率带宽，该频率带宽被分成两部分，一部分用于反向传输(移动单元到基站)，一部分用于正向传输(基站到移动单元)。为了实现双工通信，一个移动单元要使用正向和反向两个信道。传输是以直接序列扩频的形式进行的，并使用码片序列来增加数据传输的速率，进而导致信号带宽增加。采用多路存取技术将正交的码片序列分配给多个用户，因此接收者可以从多路传输中恢复自己的传输单元。

答案：(1) C　(2) A　(3) D　(4) B　(5) B

2. **参考译文：**传统的分配信号的方法，比如电话中继，多个竞争用户使用一种多路复用方案分配信道的容量，如 FDM。如果有 N 个用户，带宽将被分成 N 个同样大小的部分，每个用户将分得一部分。既然每个用户都有自己的频率范围，因此用户之间没有干扰。当用户数量少且不变，每个用户将保持稳定的数据流和通信负载，这种划分是一种简单而高效的分配机制。FM 广播电台是一个无线的例子。每个电台分配有一个 FM 频带，大部分时间用它来广播信号。但是，当发送者的数量很多且是变化的，或者通信很忙，FDM 将会有一些问题。如果频谱被分成 N 个区域，而不足 N 个用户在通信，大量宝贵的频谱会被浪费。如果超过 N 个用户想要通信，他们中一些人的通信将会因为带宽的不足而被拒绝，即使一些用户已经分配了某一频率的带宽参与过发送或接收数据。

答案：(1) B　(2) B　(3) A　(4) C　(5) D

14.3　本 章 小 结

本章要求在 2014 年的新大纲中基本没有改变，只是一些表述方式的调整。

本章要求考生具有工程师所要求的英语阅读水平以及掌握本领域的基本英语词汇。

本章内容为每次必考内容，都是以固定题型出现，分值基本保持在 10 分。考生在词汇复习中，尤其还需要注意专业词汇的缩写，这些缩写往往是某些技术、设备或协议的代称，在整个试题中是核心词汇。

14.4　达标训练题及参考答案

14.4.1　达标训练题

1.　The de facto standard application program interface (API) for TCP/IP applications is the "sockets" interface. Although this API was developed for ___(1)___ in the early 1980s. it has also

been implemented on a wide variety of non-Unix systems. TCP/IP (2) written using the sockets API have in the past enjoyed a high degree of portability and we would like the same (3) with IPv6 applications. But changes are required to the sockets API to support IPv6 and this memo describes these changes. These include a new socket address structure to carry IPv6 (4) , new address conversion functions, and some new socket options. These extensions are designed to provide access to the basic IPv6 features required by TCP and UDP applications, including multicasting, while introducing a minimum of change into the system and providing complete (5) for existing IPv4 applications.

(1) A. Windows B. Linux C. UNIX D. DOS

(2) A. applications B. networks C. protocols D. systems

(3) A. portability B. availability C. capability D. reliability

(4) A. connections B. protocols C. networks D. addresses

(5) A. availability B. compatibility C. capability D. reliability

2. Traditional IP packet forwarding analyzes the (1) IP address contained in the network layer header of each packet as the packet travels from its source to its final destination. A router analyzes the destination IP address independently at each hop in the network. Dynamic (2) protocols or static configuration builds the database needed to analyze the destination IP address (the routing table). The process of implementing traditional IP routing also is called hop-by-hop destination-based (3) routing. Although successful, and obviously widely deployed, certain restrictions, which have been realized for some time, exist for this method of packet forwarding that diminish its (4) . New techniques are therefore required to address and expand the functionality of an IP-based network infrastructure. This first chapter concentrate on identifying these restrictions and presents a new architecture, known as multiprotocol (5) switching, that provides solutions to some of these restrictions.

(1) A. datagram B. destination C. connection D. service

(2) A. routing B. forwarding C. transmission D. management

(3) A. anycast B. multicast C. broadcast D. unicast

(4) A. reliability B. flexibility C. stability D. capability

(5) A. const B. cast C. mark D. label

3. Let us now see how randomization is done when a collision occurs. After a (1) , time is divided into discrete slots whose length is equal to the worst-case round-trip propagation time on the ether(2t). To accommodate the longest path allowed by Ethernet, the slot time has been set to 512 bit times, or 51. 2μsec.

After the first collision, each station waits either 0 or 1 (2) times before trying again. If two stations collide and each one picks the same random number, they will collide again. After the second collision, each one picks either 0, 1, 2, or 3 at random and waits that number of slot times. If a third collision occurs (the probability of this happening is 0.25), then the next time the number of slots to wait is chosen at (3) from the interval 0 to 2^3-1.

In general, after i collisions, a random number between 0 and 2^i-1 is chosen, and that

number of slots is skipped. However, after ten collisions have been reached, the randomization __(4)__ is frozen at a maximum of 1023 slots. After 16 collisions, the controller throws in the towel and reports failure back to the computer. Further recovery is up to __(5)__ layers.

(1) A. datagram　B. collision　C. connection　D. service
(2) A. slot　B. switch　C. process　D. fire
(3) A. rest　B. random　C. once　D. odds
(4) A. unicast　B. multicast　C. broadcast　D. interval
(5) A. local　B. next　C. higher　D. lower

4. The TCP protocol is a __(1)__ layer protocol. Each connection connects two TCPs that may be just one physical network apart or located on opposite sides of the globe. In other words, each connection creates a __(2)__ with a length that may be totally different from another path created by another connection. This means that TCP cannot use the same retransmission time for all connections. Selecting a fixed retransmission time for all connections can result in serious consequences. If the retransmission time does not allow enough time for a __(3)__ to reach the destination and an acknowledgment to reach the source, it can result in retransmission of segments that are still on the way. Conversely, if the retransmission time is longer than necessary for a short path, it may result in delay for the application programs. Even for one single connection, the retransmission time should not be fixed. A connection may be able to send segments and receive __(4)__ faster during nontraffic period than during congested periods. TCP uses the dynamic retransmission time, a transmission time is different for each connection and which may be changed during the same connection. Retransmission time can be made __(5)__ by basing it on the round-trip time (RTT). Several formulas are used for this purpose.

(1) A. physical　B. network　C. transport　D. application
(2) A. path　B. window　C. response　D. process
(3) A. process　B. segment　C. program　D. user
(4) A. connections　B. requests　C. acknowledgments　D. datagrams
(5) A. long　B. short　C. fixed　D. dynamic

14.4.2　参考答案

1. (1) C　(2) A　(3) A　(4) D　(5) B

参考译文：对于 TCP/IP 应用，事实上的应用程序接口(API)标准是“套接字”接口。虽然这个 API 是在 20 世纪 80 年代早期为 UNIX 开发的，但是也广泛地在各种非 UNIX 系统中得到了实现。以前采用套接字 API 编写的 TCP/IP 应用具有高度的兼容性，因而我们也希望对 IPv6 应用具有同样的兼容性。为了支持 IPv6，需要对套接字 API 作出某些改变，这个便笺就是描述这些变化的。这些改变包括一种新的用于支持 IPv6 地址的套接字地址结构、新的地址转换功能以及新的套接字选项。这些扩展可以满足 TCP 和 UDP 应用访问 IPv6 基本功能(包括组播)时的需要，但是只对系统进行了最小的改变，而且与现有的 IPv4 应用是完全兼容的。

2. (1) B (2) A (3) D (4) B (5) D

参考译文：传统的IP分组转发机制是在分组从源端到达最终目标的旅行过程中，分析包含在每个分组网络层头部的目标IP地址字段。在网络的每一跳步中，路由器独立地分析y标IP地址字段。动态路由协议或者静态配置都建立了用于分析目标IP地址字段的数据库(路由表)。实现传统IP路由的过程也被叫作逐跳的基于目标的单播路由。虽然这种分组转发技术已经取得了成功并被广泛地部署在网络中，然而人们早已认识到，还存在一些约束条件降低了它的灵活性。因而需要一种新技术来改进和扩展基于IP的网络架构功能。这一章集中于识别这些约束条件，并提出一种新的体系结构，这就是多协议标记交换技术，它提供了克服这些约束条件的解决方案。

3. (1) B (2) A (3) B (4) D (5) C

参考译文：现在让我们观察冲突发生时如何做随机处理。冲突发生后，时间被划分成离散的长度等于最坏的往返传播时间的时槽。为了容纳以太网允许的最长路径，冲突时槽缩小为51.2μs。

第一次冲突后，每个站再次尝试前需要等待0或1时槽。如果每一站发生冲突，且每一站挑选相同的随机数，它们将再次发生冲突。第二次冲突之后，每一站随机选择0、1、2或3，等待时槽的个数。如果第三次冲突发生(发生的概率为0.25)，则下次时槽的等待数量都是在$0 \sim 2^3-1$随机挑选的。

总的来说，第i次冲突后，将在$0 \sim 2^i-1$挑选随机数，而且那个时槽数是被略过的。然而，当冲突次数达到10次，随机间隔被锁定在最高1023时槽。当16次冲突后，控制器丢弃报告而没有返回计算机。进一步恢复已经达到更高的层次。

4. (1) C (2) A (3) B (4) C (5) D

参考译文：TCP是一种传输层协议。每一个连接都连接了两个TCP实体，这两个TCP实体可能存在于同一个物理网络中，也可能是分居于地球的两边。换言之，每一个连接都产生了一条通路，其长度与另外一个连接产生的通路完全不同。这就意味着，TCP不能对所有的连接使用同样的重传时间。对所有的连接选择一个固定的重传时间可能产生严重的后果。如果重传时间不足以使一个段到达目标，或者不足以使一个应答到达源站，这就可能对尚在路途中的段产生重传。反之，如果重传时间比一条短通路所需要的时间长，则可能对应用程序产生延迟。

即使对单个连接，重传时间也不应该固定。一个连接应该能够在非峰值时段比拥堵时段更快地发送数据段和接收应答。TCP使用了动态重传时间，重传时间对每一个连接是不同的，在同一个连接持续期间也是可以改变的。重传时间可以动态地根据环回时间(RTT)而改变。为此建立了几个有用的公式。

参 考 文 献

[1] 特南鲍姆，韦瑟罗尔著. 计算机网络[M]. 5 版. 严伟，潘爱民译. 北京：清华大学出版社，2012.

[2] 谢希仕. 计算机网络[M]. 7 版. 北京：电子工业出版社，2017.

[3] 雷震甲. 网络工程师教程[M]. 5 版. 北京：清华大学出版社，2018.

[4] 王达. 华为交换机学习指南[M]. 北京：人民邮电出版社，2013.

[5] 刘永华，孟凡楼等著. Windows Server 2008 网络操作系统[M]. 北京：清华大学出版社，2017.